



D-Link DSL-2750B Wireless Gateway

User Guide

Table of Contents



| | |
|--|-----------|
| Product Overview | 5 |
| Product Description | 5 |
| Safety Instructions | 5 |
| Networking Requirements | 6 |
| Hardware Features..... | 7 |
| LED Indicators | 7 |
| Ports/Buttons..... | 7 |
| Installation | 8 |
| DSL Filters/Microfilters | 8 |
| Configure your Computer | 8 |
| Windows® 8/7/Vista®/XP/2000 | 8 |
| Mac OS® X | 9 |
| Connect your Gateway..... | 10 |
| Web-based Configuration Utility | 11 |
| Wireless..... | 13 |
| Overview | 13 |
| Settings..... | 14 |
| Wireless..... | 15 |
| Wireless Network Settings | 16 |
| MAC Filtering | 17 |
| WPS..... | 18 |
| WPA/WPA2 Security..... | 19 |
| WEP Security | 20 |
| 802.1x Authentication | 21 |
| Advanced | 22 |
| My Network..... | 23 |
| Overview | 23 |
| Internet | 24 |
| LAN..... | 25 |
| General..... | 25 |
| Settings | 27 |
| Internet Protocol..... | 29 |
| DNS Server..... | 29 |
| IP Address Distribution (DHCP) | 30 |
| DHCP Server Pools (DHCP Reservation)..... | 31 |
| Routing | 32 |
| Bridging | 33 |
| Advanced | 34 |

| | |
|--------------------------------------|----|
| Firewall Settings | 35 |
| Overview | 35 |
| Access Control | 36 |
| Port Forwarding | 37 |
| DMZ Host | 39 |
| Port Triggering..... | 40 |
| Connections | 41 |
| Advanced Filtering..... | 42 |
| Remote Administration..... | 43 |
| Security Log..... | 44 |
| Settings | 45 |
| System Log | 46 |
| Services..... | 47 |
| Overview | 47 |
| QoS..... | 48 |
| Overview | 48 |
| Utilization by Computer..... | 49 |
| Utilization by Application..... | 49 |
| Traffic Priority | 50 |
| Traffic Shaping..... | 51 |
| DSCP Settings | 52 |
| 802.1p Settings | 53 |
| Class Statistics..... | 54 |
| Parental Controls | 55 |
| Overview | 55 |
| Filtering Policy | 56 |
| Advanced Options | 58 |
| Statistics..... | 59 |
| Storage..... | 60 |
| File Server | 60 |
| Disk Management..... | 61 |
| Personal Domain Name (DDNS) | 62 |
| IP Address Distribution (DHCP) | 63 |
| System..... | 64 |
| Overview | 64 |
| Settings | 65 |
| Date and Time..... | 66 |
| Users..... | 67 |
| Overview | 67 |
| RADIUS Client | 68 |
| Network Connections..... | 69 |

| | |
|--|-----------|
| Monitor | 70 |
| Network | 70 |
| CPU | 70 |
| Routing | 71 |
| Overview | 71 |
| PPPoE Relay | 71 |
| Universal Plug and Play (UPnP™) | 72 |
| Maintenance | 73 |
| Reboot..... | 73 |
| Restore Factory Settings | 73 |
| Firmware Upgrade | 74 |
| Diagnostics | 75 |
| Objects and Rules..... | 76 |
| Protocols..... | 76 |
| Network Objects..... | 77 |
| Scheduler Rules..... | 78 |
| Certificates | 79 |
| Advanced Configuration | 80 |
| Bridge Mode | 80 |
| Multiple Static Public IPs..... | 83 |
| Connect to your Wireless Network..... | 86 |
| Windows® 8 | 86 |
| Windows® 7 | 88 |
| Windows Vista® | 90 |
| Windows® XP | 91 |
| Networking Basics | 92 |
| Check your IP address..... | 92 |
| Windows® 8 Users | 92 |
| Windows® 7/Vista® Users | 92 |
| Windows® XP Users | 92 |
| Statically Assign an IP Address | 93 |
| Windows® 8 Users..... | 93 |
| Windows® 7/ Vista® Users..... | 94 |
| Windows® XP Users | 95 |

Product Overview

Product Description

The Verizon® D-Link® DSL-2750B Wireless Gateway provides reliable, high-speed, Internet access to your existing small office phone line and is capable of data rates hundreds of times faster than a traditional analog modem. But unlike analog modems, the Gateway allows you to use the same phone line for simultaneous voice/fax communications and high-speed Internet access, eliminating the need for dedicated phone lines for voice and data needs. In addition, it supports a variety of networking interfaces along with the following optional features:

- Four 10/100 Ethernet Ports
- 802.11n wireless technology to provide the best wireless performance
- Advanced firewall features including parental control, access control, and content filtering
- Wi-Fi Protected Setup (WPS) Push Button/PIN setup
- UPnP Support
- USB port for sharing music/video/images using a thumb drive or external hard drive

Safety Instructions

- Never install any telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch non-insulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.

WARNING: Risk of electric shock. Voltages up to 140 Vdc (with reference to ground) may be present on telecommunications circuits.



Networking Requirements

The following system specifications are required for optimum performance of the Router via 10/100 Ethernet or 802.11n/g wireless.

ETHERNET:

- Pentium® or equivalent class machines or higher
- Microsoft® Windows® (8, 7, Vista®, XP, 2000, ME, NT 4.0, 98 SE) Mac OS® X, or Linux installed
- 64 MB RAM (128 MB recommended)
- 10 MB of free hard drive space
- 10/100 Base-T Network Interface Card (NIC)
- Internet Explorer® 6.0, Firefox® 3.0, Safari® 3.0 or Chrome 2.0 or higher

WIRELESS:

- Pentium® or equivalent class or higher
- Microsoft® Windows® (8, 7, Vista®, XP, 2000) or Mac OS® X installed
- 64 MB RAM (128 MB recommended)
- 10 MB of free hard drive space
- Internet Explorer® 6.0, Firefox® 3.0, Safari® 3.0 or Chrome 2.0 or higher
- Available IEEE 802.11n/g wireless clients

LED Indicators

This section explains the LED states and descriptions. LED indicators are used to verify the unit's operation and status.

| | | |
|----------|-----------------------|---|
| 1 | Power | A solid green light indicates the unit is powered on. A red light indicates a malfunction. |
| 2 | Ethernet (1-4) | A solid light indicates a connection to an Ethernet-enabled computer on ports 1-4. This LED blinks during data transmission. |
| 3 | Wireless | A solid green light indicates the wireless function is operating correctly. A flashing green light indicates wireless traffic is passing through the router. |
| 4 | USB | A solid green light indicates a good connection to a USB device. This light will blink during data transmission. |
| 5 | DSL | A solid light indicates the DSL is synchronized. A flashing LED indicates the modem is attempting to synchronize with the DSL provider. |
| 6 | Internet | A solid green light indicates that the modem has an IP address and is connected to the Internet. A red light indicates that the modem does not have an IP address or authentication has failed. No light indicates that an ADSL connection is not present or the modem is in bridge mode. |

Ports/Buttons

The following chart displays the Router's connector types:

| | | |
|----------|------------------------|--|
| 1 | DSL Port | Connect to an active telephone line (RJ-11). |
| 2 | LAN Ports (1-4) | Connect Ethernet devices such as computers, switches, and hubs. |
| 3 | USB Port | Connect a USB thumb drive or external hard drive and share files with users on your network. |
| 4 | WLAN Button | Pressing this button to turn the Wireless feature on or off. |
| 5 | Reset Button | Pressing the Reset button for 10 seconds restores the modem to its original factory default settings. |
| 6 | ON/OFF | Press this button to turn the unit on or off. |
| 7 | Power Receptor | Receptor for the supplied power adapter. |
| 8 | WPS Button | Press the WPS button located on the side to add your device to an existing network or to create a new network. |

This section will explain how to configure your computers to connect to the gateway, configure the gateway to connect to the Internet, and set up your wireless clients.

DSL Filters/Microfilters

ADSL signals must be blocked from reaching each telephone, answering machine, fax machine, or any similar conventional device. Failure to do so may degrade telephone voice quality and ADSL performance.

Install a microfilter if you desire to use the DSL-equipped line jack for telephone, answering machine, fax machine or other telephone device connections. Microfilter installation requires no tools or telephone rewiring. Just unplug the telephone device from the baseboard or wall mount and plug in a microfilter and then plug in the telephone device.

You can purchase microfilters from your local electronics retailer, or contact the original provider of your DSL equipment.

Configure your Computer

Windows® 8/7/Vista®/XP/2000

Follow the steps below to configure your computer to automatically receive its IP settings from the Gateway:

1. Windows® 8 - Press the **Windows** key and then type **IP**. Click **Settings** on the right side and then click **View Network Connections**.
Windows® 7 - Click on **Start > Control Panel > Network and Internet > Network and Sharing Center**.
Windows Vista® - Click on **Start > Control Panel > Network and Internet > Network and Sharing Center > Manage Network Connections**.
Windows® XP - Click on **Start > Control Panel > Network Connections**.
Windows® 2000 - From the desktop, right-click **My Network Places > Properties**.
2. Right-click on the **Local Area Connection** which represents your D-Link network adapter and select **Properties**.
3. Highlight **Internet Protocol (TCP/IP)** or **Internet Protocol Version 4 (TCP /IPv4)** and click **Properties**.
4. In the Internet Protocol (TCP/IP) Properties dialog box, click on the radio buttons labeled **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
5. Click **OK** twice to save your settings.

Below are instructions for configuring your Mac OS® X operating system

1. In the Mac OS X Dock, click on the **System Preferences** icon.
2. Under **Internet & Network**, click **Network**. In the **Show** menu, select **Built-in Ethernet** or Ethernet (Depending on your Mac OS version.)
3. Click the **TCP/IP** tab.
4. In the Configure menu, select **Using DHCP**.
5. Click **Apply Now and Save** if your computer prompts you to save changes.

If you want to assign a static IP address, please use the settings below:

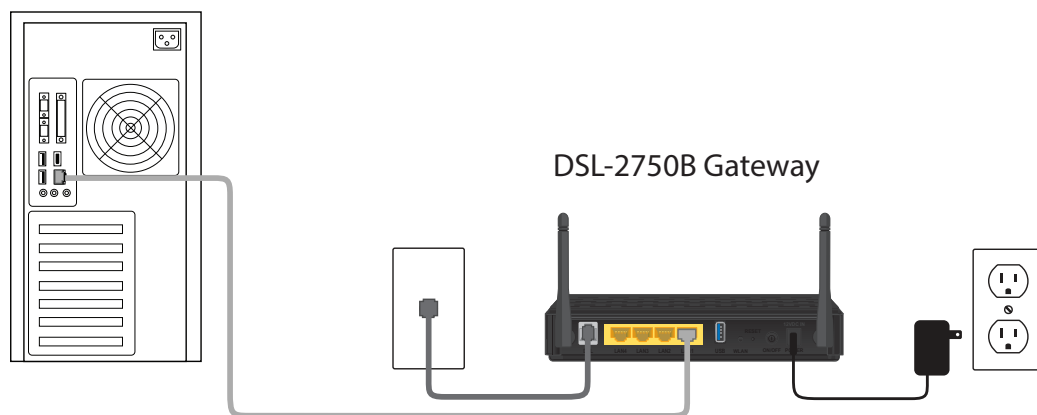
- Your PC's TCP/IP address: 192.168.1.x (where "x" is any number between 2 and 254)
- The Default Gateway's IP address: 192.168.1.1
- Subnet mask: 255.255.255.0
- DNS server: 192.168.1.1 (same IP as the Gateway) or supplied by Verizon

Connect your Gateway



1. Connect an RJ-11 (phone) cable from your wall phone jack to the DSL port on the back of the DSL-2750B gateway.
2. Connect an Ethernet cable from the LAN1 port on the back of the DSL-2750B to the Ethernet port on your computer.
3. Connect the supplied power adapter into the power receptor on the back of the DSL-2750B gateway to a power outlet or a surge protector (recommended).
4. Once you connect the power adapter, press the ON/OFF button on the back of the gateway to turn the unit on.

Desktop Computer

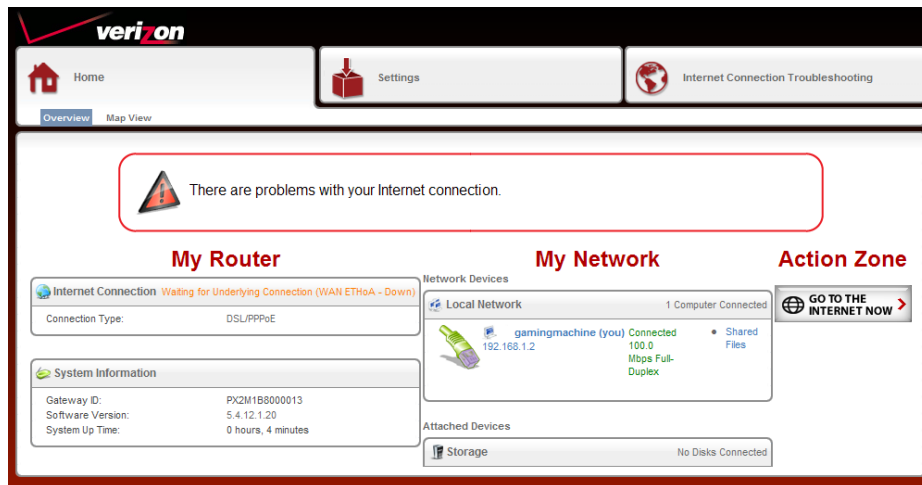


Web-based Configuration Utility

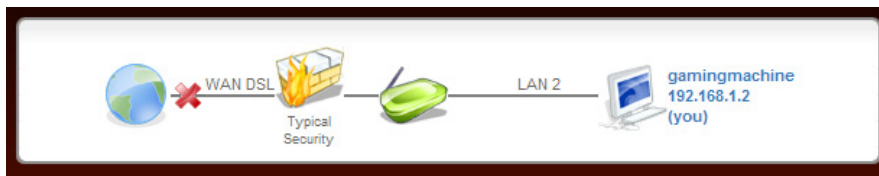


To log into the gateway, follow the steps below:

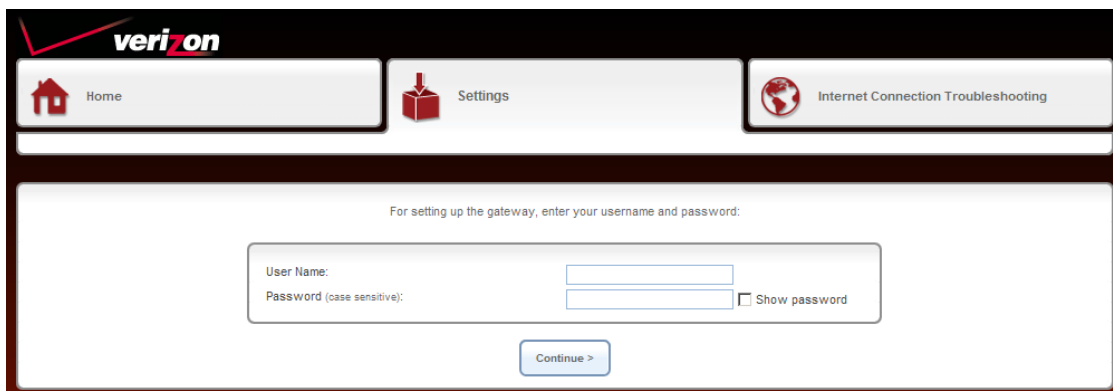
1. Launch your web browser such as Internet Explorer.
2. In the address bar enter **http://192.168.1.1** and press **Enter**.
3. The Home page will appear. The **Overview** screen displays the gateway status summary in one convenient location. The user can quickly and efficiently view important details of the connection status and hardware peripherals, as well as the status of different services. If you click any other link/tab, you will be asked to log in.



Map View depicts the various network elements, such as the Internet connection, firewall, gateway, internal network interface (Ethernet, USB, and Wireless), and local network computers and peripherals visually.

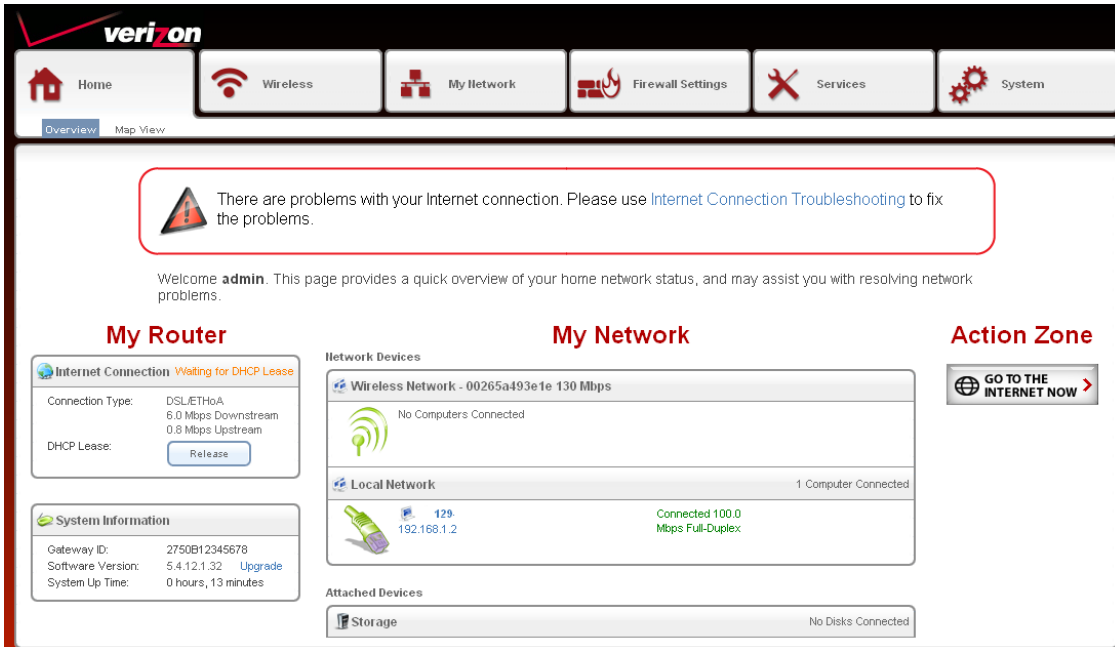


4. Click **Settings** to configure your router. Once the login screen appears, enter **Admin** next to *Username* and then enter your password (refer to “login password” on the label located on the bottom of the Gateway). Click **Continue**.



The **Home > Overview** screen will appear. This screen gives you an overview of your Gateway including the Internet connection status, system information, local network information, and storage status.

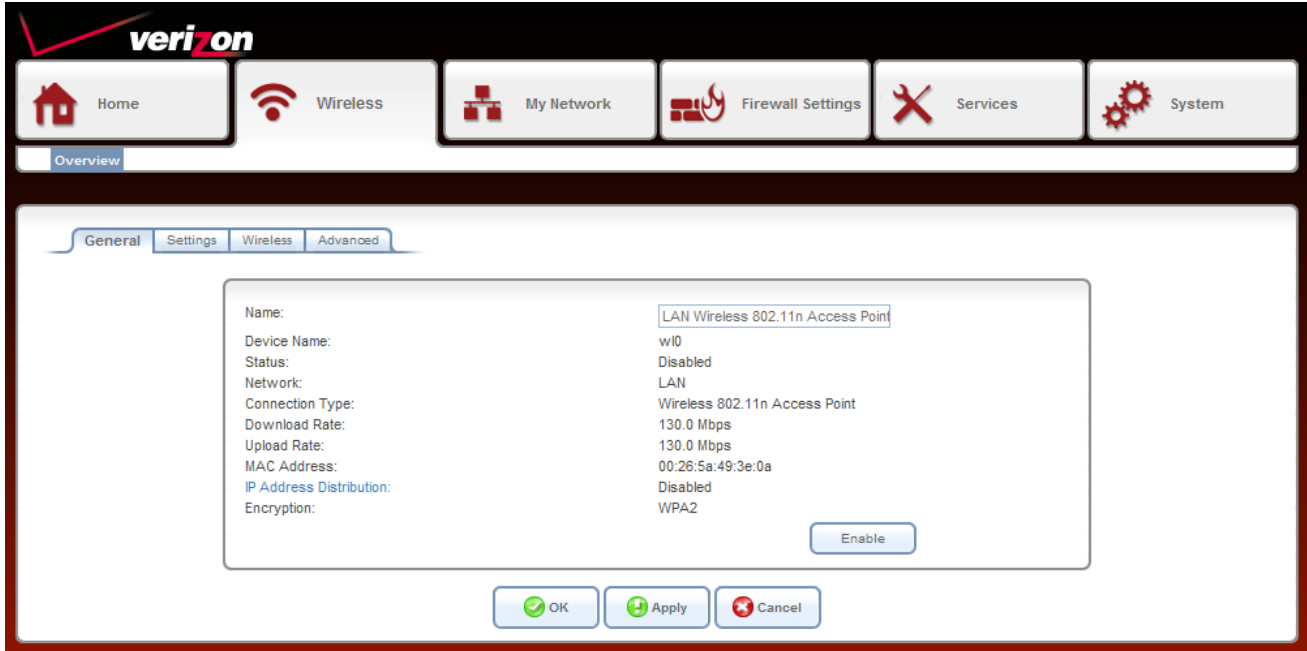
When the router is configured with DHCP, you will be able to Release and Renew your WAN IP Address with the buttons located here.



Wireless Overview

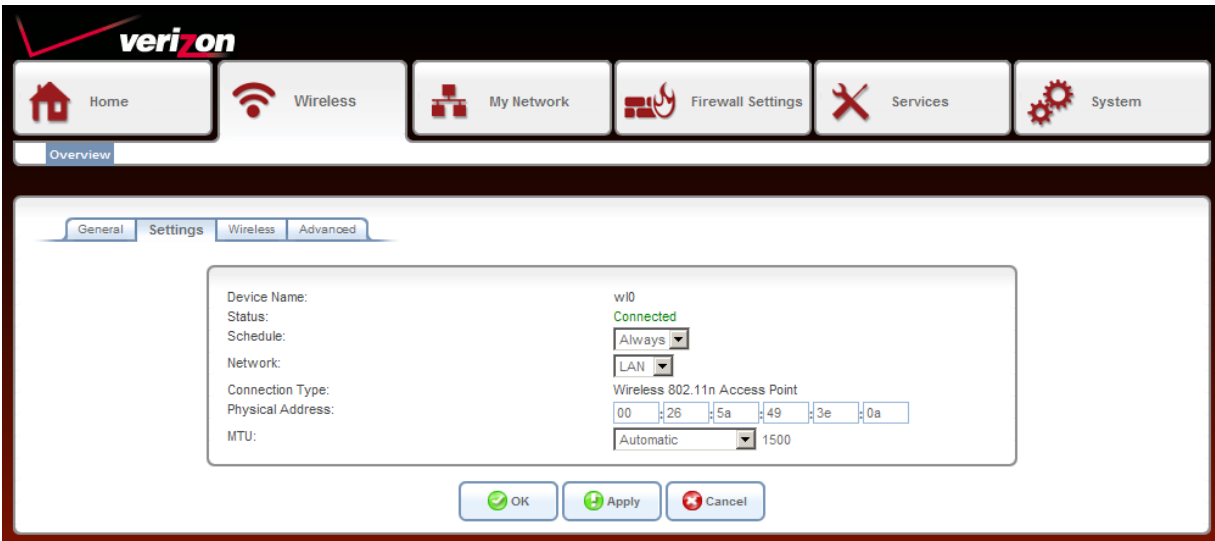


The **Wireless > Overview** screen displays the Gateway's current wireless settings.



Enable Button: Click the Enable button to turn on the wireless function.

The **Wireless > Settings** screen allows you to change the Gateway's wireless settings.



Device Name: Displays the name of the Interface.

Status: Displays the current connection state.

Schedule: Select a time frame from the drop-down menu to have the wireless function active.

Network: LAN is selected.

Connection Type: Displays the wireless mode the Gateway is set to.

Physical Address: Displays the MAC address of the Gateway (wireless side).

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.

The **Wireless > Wireless** screen allows you to change the Gateway's wireless network settings.

The screenshot displays the Verizon DSL-2750B user interface for wireless settings. At the top, there is a navigation bar with icons for Home, Wireless, My Network, Firewall Settings, Services, and System. Below this is an 'Overview' section with tabs for General, Settings, Wireless, and Advanced. The main content area is divided into several sections:

- Wireless Network (SSID):** A text input field containing '00265a493e08'. Below it is a checked checkbox for 'SSID Broadcast'.
- 802.11 Mode:** A dropdown menu set to '802.11b/g/n'.
- Channel (FCC):** A dropdown menu set to 'Automatic', with '11 - 2.462GHz' displayed next to it.
- Channel Width Mode:** A dropdown menu set to '20 MHz only'.
- Network Authentication:** A dropdown menu set to 'Open System Authentication'.
- MAC Filtering:** A dropdown menu set to 'Disable'.
- WPS:** A checked checkbox for 'Enabled'. Below it, 'Access Point Pin Code' is 'Ready', 'Status' is 'Ready', and 'Protected Setup Method' is 'Push Button'. A 'Go' button is present.
- Security:** A dropdown menu set to 'WPA2'. Below it, 'Authentication Method' is 'Pre-Shared Key', 'Advanced WPA' is unchecked, and there are four input fields containing '1234', '5678', '90AB', and 'CDEF'. 'Encryption Algorithm' is 'AES', and 'Group Key Update Interval' is '900' seconds.
- Transmission Rate:** A dropdown menu set to 'Auto'.
- Transmit Power:** A dropdown menu set to '100 %'.
- CTS Protection Mode:** A dropdown menu set to 'Auto'.
- CTS Protection Type:** A dropdown menu set to 'cts-only'.
- Frame Burst - Max Number:** An input field with '3'.
- Frame Burst - Burst Time:** An input field with '2'.
- Beacon Interval:** An input field with '100' ms.
- DTIM Interval:** An input field with '3' ms.
- Fragmentation Threshold:** An input field with '2346'.
- RTS Threshold:** An input field with '2347'.
- Virtual APs:** A table with columns: Name, BSSID, SSID, Status, and Action.

| Name | BSSID | SSID | Status | Action |
|---|-------------------|--------------|-----------|--------|
| LAN Wireless 802.11n Access Point New Virtual AP | 00:26:5a:49:3e:0a | 00265a493e08 | Connected | |

At the bottom of the page, there are three buttons: 'OK', 'Apply', and 'Cancel'.

Wireless Network Settings



| | |
|--|---|
| Wireless Network (SSID): | <input type="text" value="p0265a493e08"/> |
| <input checked="" type="checkbox"/> SSID Broadcast | |
| 802.11 Mode: | <input type="text" value="802.11b/g/n"/> |
| Channel (FCC): | <input type="text" value="Automatic"/> 11 - 2.462GHz |
| Channel Width Mode: | <input type="text" value="20 MHz only"/> |
| Network Authentication: | <input type="text" value="Open System Authentication"/> |

Wireless Network Service Set Identifier (SSID) is the name of your wireless network. Create a name using up to 32 (SSID): characters. The SSID is case-sensitive. For security reasons, do not choose a name with personal information.

SSID Broadcast: When this box is checked, the SSID (name of your wireless network) will broadcast. Wireless clients within range of your Gateway will be able to see your network. For added security, you may uncheck this box but will have to manually enter the SSID on your wireless clients.

802.11 Mode: Select the type of wireless clients that will connect to your wireless network.
802.11b/g Mixed - Select if you are using a mix of 802.11b and 11g wireless clients.
802.11g Only - Select if all of your wireless clients are 802.11g.
802.11b Only - Select if all of your wireless clients are 802.11b.
802.11b/g/n - Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.
802.11n Only - Select only if all of your wireless clients are 802.11n.
802.11g/n - Select if you are using a mix of 802.11n and 11g wireless clients.

Channel (FCC): Select the wireless channel. It is strongly recommended to select **Automatic**.

Channel Width Select the Channel Width:

Mode: **20MHz** - This is the default setting. Select if you are not using any 802.11n wireless clients.
20/40MHz (dynamic) - Select if you are using both 802.11n and non-802.11n wireless devices.
40MHz - Select if using only 802.11n wireless clients.

Network Authentication: Select the authentication mode from the drop-down. **Open System** is the default settings. When using WEP encryption, it is recommended to select **Shared Key**.

MAC Filtering



Use MAC (Media Access Control) Filtering to allow or deny wireless computers and devices by their MAC addresses from accessing the Network. You will need to manually add the MAC address of your wireless client you want to filter.

| MAC Address | Action |
|---------------------------------|--------|
| New MAC Address | |

MAC Filtering: Select from the drop-down menu:

Disable - turn off MAC filtering.

Allow - Allows only the computers/devices you want from your network to access the Internet. All other computers will be blocked if not added.

Deny - Blocks computers/devices you want from your network from accessing the Internet. All other computers will be allowed to connect.

Action/New MAC Click the green + icon or **New MAC Address** to add your wireless clients. To find the MAC address **Address:** on a computer, please refer to the Networking Basics section in this manual.

Add New MAC Address

Step 1: Click the green + icon under *Action*.

Step 2: Enter the MAC Address of your computer or device and click **OK**.

MAC Address: 00 : 3c : ab : 00 : 12 : 6d

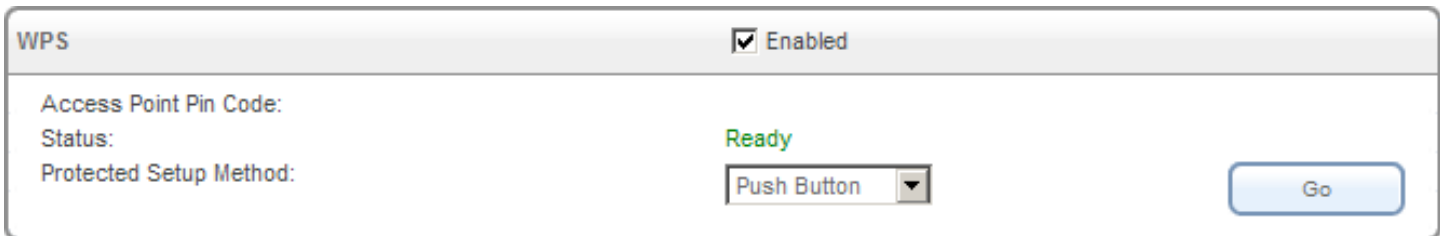
OK Cancel

Step 3: Your newly added device will now be displayed in the list. Click the red X to remove the device from the list. To add more, repeat steps 1 and 2.

| MAC Address | Action |
|---------------------------------|--------|
| 00:3c:ab:00:12:6d | |
| New MAC Address | |

Wi-Fi Protected Setup (WPS) System is a simplified method for securing your wireless network during the “Initial setup” as well as the “Add New Device” processes. The Wi-Fi Alliance (WFA) has certified it across different products as well as manufactures. The process is just as easy, as pressing a button for the Push-Button Method or correctly entering the 8-digit code for the Pin-Code Method. The time reduction in setup and ease of use are quite beneficial, while the highest wireless Security setting of WPA2 is automatically used.

Push Button



The screenshot shows the WPS configuration page. At the top, there is a header with 'WPS' on the left and a checked checkbox labeled 'Enabled' on the right. Below this, the 'Access Point Pin Code:' field is empty. The 'Status:' is displayed in green text as 'Ready'. The 'Protected Setup Method:' is set to 'Push Button' in a dropdown menu. A 'Go' button is located on the right side of the form.

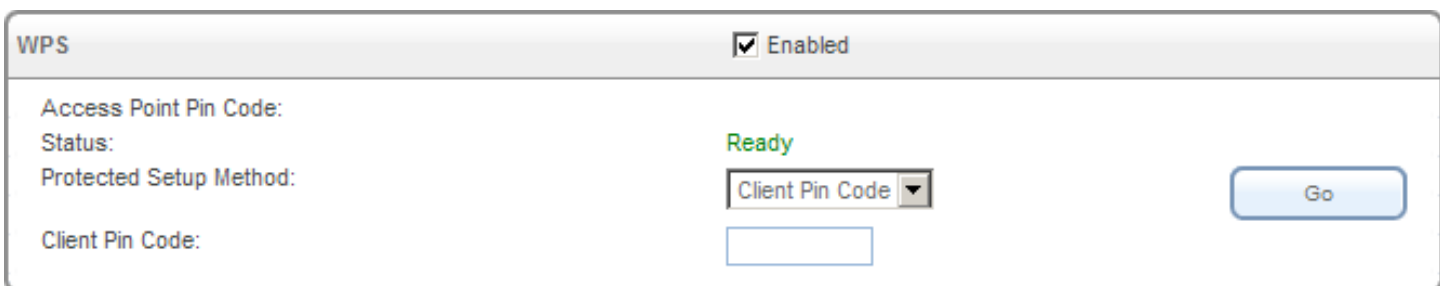
Step 1: Select **Push Button** from the drop-down and then click the **Go** button to start the WPS process.

Step 2: Within 2 minutes, press the WPS button on your wireless client. Some clients may require you to launch its software utility and click a WPS button. Please refer to your wireless client’s user guide for more information.

Step 3: Allow 1-2 minutes for the devices to communicate. Once complete your client will connect to the gateway.

Client PIN Code

A PIN is a unique number that can be used to add the router to an existing network or to create a new network. You will need to get the PIN number from one of your wireless clients. Please refer to your wireless client’s user guide for more information.



The screenshot shows the WPS configuration page. At the top, there is a header with 'WPS' on the left and a checked checkbox labeled 'Enabled' on the right. Below this, the 'Access Point Pin Code:' field is empty. The 'Status:' is displayed in green text as 'Ready'. The 'Protected Setup Method:' is set to 'Client Pin Code' in a dropdown menu. Below this, there is an empty text input field for the 'Client Pin Code:'. A 'Go' button is located on the right side of the form.

Step 1: From your wireless client, write down the PIN and activate/start the WPS process.

Step 2: Within 2 minutes from the Gateway, select **Client Pin Code** from the drop-down, enter the PIN number in the box, and then click the **Go** button.

Step 3: Allow 1-2 minutes for the devices to communicate. Once complete your client will connect to the gateway.

WPA/WPA2 Security



This section will allow you to secure your wireless network using WEP, WPA, or WPA2 encryption. When using these options, you must disable WPS. Refer to the previous page and uncheck the WPS box.

The default setting and recommended level of security is WPA2.

| | |
|---|--|
| Security | WPA2 |
| Authentication Method: | Pre-Shared Key |
| Pre-Shared Key: | <input type="checkbox"/> Advanced WPA 1234 5678 90AB CDEF |
| Encryption Algorithm: | AES |
| <input checked="" type="checkbox"/> Group Key Update Interval | 900 Seconds |

Authentication Method: Select **WPA** or **WPA2**.

Advanced WPA: Check this box to change the pre-shared key (passphrase).

Pre-Shared Key: Displays the current WPA/WPA2 passphrase.

Encryption Algorithm: Select **AES**, **TKIP**, or **AES and TKIP**.

Group Key Update Interval: Enter the amount of time before the group key used for broadcast and multicast data is changed.

WEP Security



WEP is an older, less-secure encryption option. It is strongly recommended to use WPA or WPA2.

| Security | |
|----------|-------|
| | WEP ▼ |

| WEP Keys | | | |
|------------------------------------|----------------------|--------------|------------|
| Active | Encryption Key | Entry Method | Key Length |
| <input checked="" type="radio"/> 1 | <input type="text"/> | ASCII ▼ | 104 bit ▼ |
| <input type="radio"/> 2 | <input type="text"/> | ASCII ▼ | 40 bit ▼ |
| <input type="radio"/> 3 | <input type="text"/> | ASCII ▼ | 40 bit ▼ |
| <input type="radio"/> 4 | <input type="text"/> | ASCII ▼ | 40 bit ▼ |

Authentication Select **WEP** from the drop-down menu.

Method:

WEP Keys: You may enter up to 4 different keys. Select the key you want to use.

Encryption Key: Enter a WEP key.

Entry Method: Select the type of key from the drop-down menu.

Hex - letters A-F and numbers 0-9 are valid.

ASCII - all letters and numbers are valid.

Key Length: Select the level of encryption (40 or 104-bit).

802.1x Authentication



This section will allow you to secure your wireless network using 802.1x authentication. When using this option, you must disable WPS.

| | |
|---|---------------|
| WPS <input type="checkbox"/> Enabled | |
| Security WPA | |
| Authentication Method: | 802.1X |
| Encryption Algorithm: | TKIP and AES |
| <input checked="" type="checkbox"/> Group Key Update Interval | 900 Seconds |
| RADIUS Server | |
| Server IP: | 0 . 0 . 0 . 0 |
| Server Port: | |
| Shared Secret: | |

Authentication Method: Select **802.1x WEP, WPA** or **WPA2**.

Encryption Method: If you selected WPA or WPA2, you will need to select 802.1x from the drop-down menu.

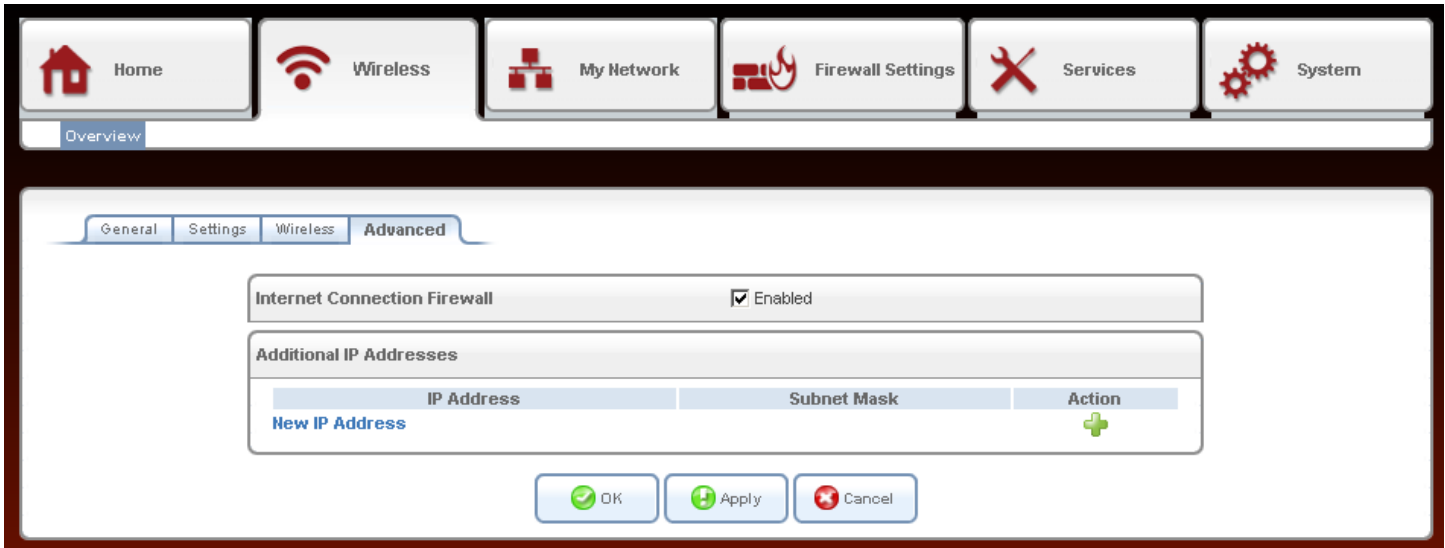
Encryption Algorithm: If you selected WPA or WPA2, Select the type of encryption you want to use - **AES, TKIP**, or **AES and TKIP**.

Group Key Update Interval: Enter the amount of time before the group key used for broadcast and multicast data is changed.

Server IP: Enter the IP address of the RADIUS server.

Server Port: Enter the port you want to use.

Shared Secret: Enter the Shared Secret passphrase.



Home Wireless My Network Firewall Settings Services System

Overview

General Settings Wireless **Advanced**

Internet Connection Firewall Enabled

Additional IP Addresses

| IP Address | Subnet Mask | Action |
|--------------------------------|-------------|--------|
| New IP Address | | |

OK Apply Cancel

Internet Connection Firewall: Check the Enable box to enable the firewall feature for your wireless computers/devices.

New IP Address: Click to add a new device.

IP Address: The IP address of the computer or device.

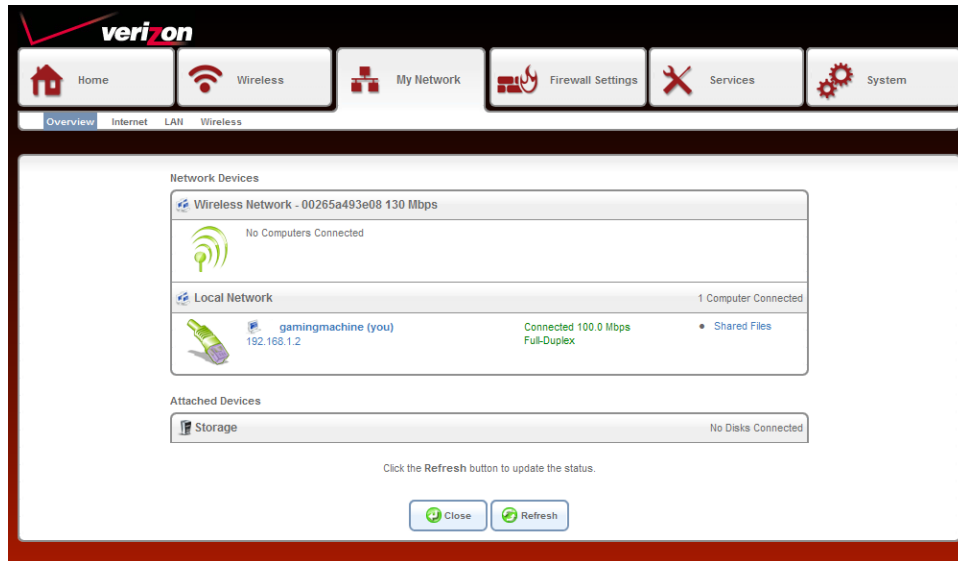
Subnet Mask: The subnet mask of the computer or device.

Action: Click the green + sign to add a computer or device, or click the red X to delete the computer or device.

My Network Overview



The **My Network > Overview** screen displays your network devices on your network and any attached storage devices.



Wireless Network: This section will display any wireless device connected to your Gateway.

Local Network: This section will display any Ethernet device connected to your Gateway.

You can click the computer name, IP address or “Shared Files” to access any shares on that computer.

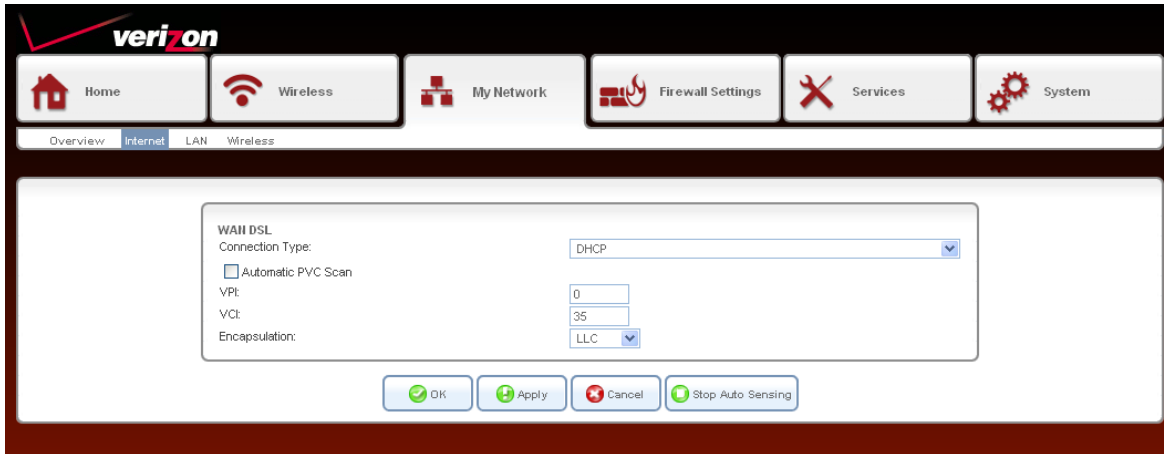
Attached Devices: This section will display if any USB storage devices (thumb drive/external hard drive) are connected to your Gateway.

Internet



The **My Network > Internet** screen allows you to change your Internet settings. This section should only be configured by Verizon technicians.

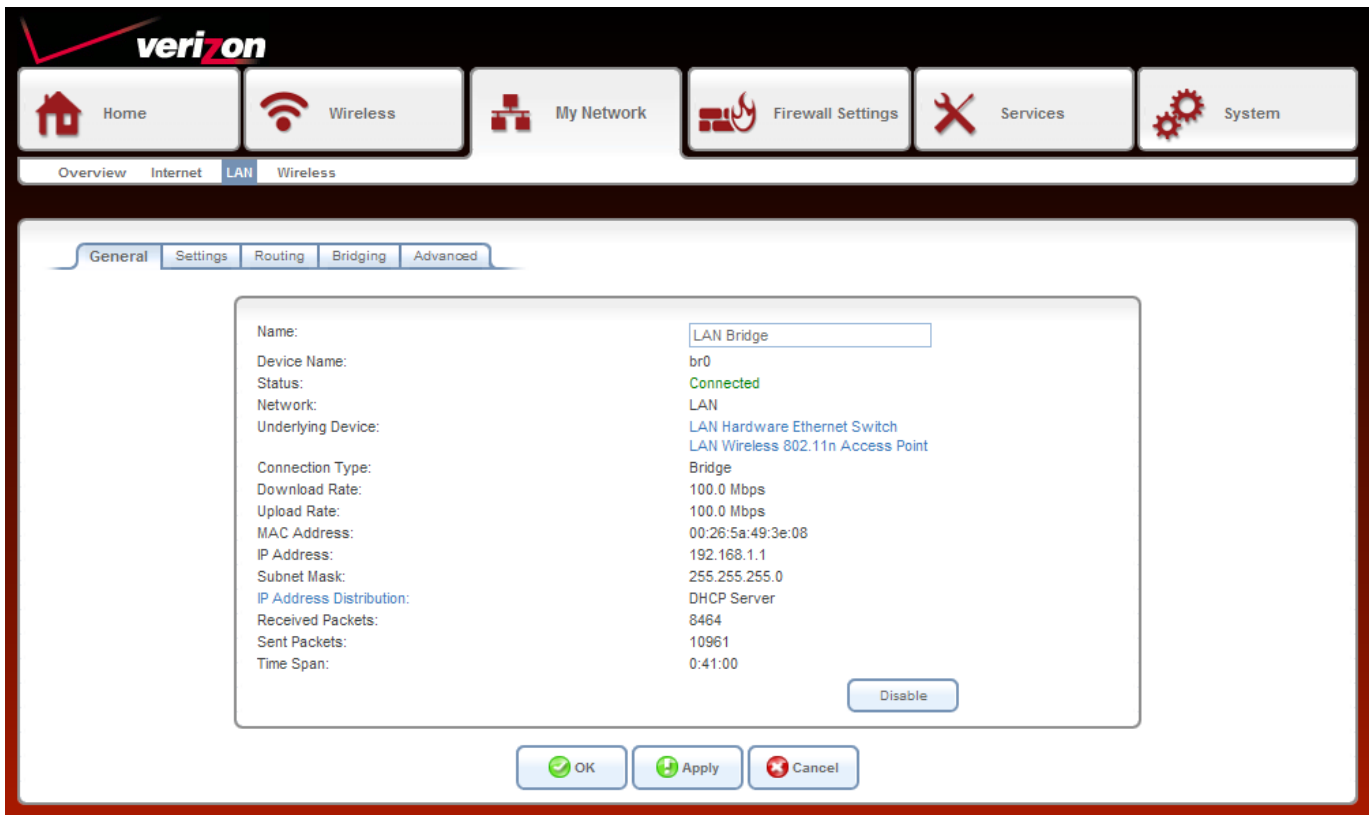
Auto-Sense will automatically detect your Internet settings. It is not recommended to manually make changes to your Internet settings. However, if you choose to do so, you must disable Auto-Sense by clicking the Stop Auto-Sense button from this page. Note: Once you disable Auto-Sense, you can only re-enable it by restoring factory settings.



LAN General



The **My Network > LAN** screen displays a summary of the Gateway's local (router) settings.



Name: The name of the LAN side of the Gateway.

Device Name: Displays the name of the Interface.

Status: The current status of the LAN side of the Gateway.

Underlying Device: You may click **LAN Hardware Ethernet Switch** or **LAN Wireless 802.11n Access Point** to configure their settings.

Connection Type: Displays the connection type.

Download Rate: Displays the Ethernet download speed.

Upload Rate: Displays the Ethernet upload speed.

MAC Address: The MAC address of the LAN side of the Gateway.

IP Address: The IP address of the LAN side of the Gateway.

Subnet Mask: The subnet mask of the Gateway.

IP Address Distribution: Click to change the DHCP settings.

Distribution:



Received Packets: Amount of packets received.

Sent Packets: Amount of packets sent.

Time Span: Displays the time connected.

Disable Button: Click to disable the use of the Ethernet ports (LAN) on your Gateway.

Settings



This section allows you to change the network settings (LAN) of your Gateway.

The screenshot displays the Verizon Gateway's LAN settings interface. At the top, there is a navigation bar with icons for Home, Wireless, My Network, Firewall Settings, Services, and System. Below this is a sub-navigation bar with tabs for Overview, Internet, LAN (selected), and Wireless. The main content area is titled 'LAN' and contains several configuration sections:

- General Settings:** Device Name: br0; Status: Connected; Schedule: Always; Network: LAN; Connection Type: Bridge; Physical Address: 10.26.5a.49:3e:08; MTU: Automatic (1500).
- Internet Protocol:** Use the Following IP Address; IP Address: 192.168.1.1; Subnet Mask: 255.255.255.0.
- DNS Server:** Use the Following DNS Server Addresses; Primary DNS Server: 0.0.0.0; Secondary DNS Server: 0.0.0.0.
- IP Address Distribution:** DHCP Server; Start IP Address: 192.168.1.1; End IP Address: 192.168.1.254; Subnet Mask: 255.255.255.0; WINS Server: 0.0.0.0; Lease Time in Minutes: 60. Checkboxes for 'Provide Host Name If Not Specified by Client' and 'Provide DNS Server to Clients' are checked.
- DHCP Server Pools:** A table with columns for Criteria, Dynamic IP Range, and Action. A 'New IP Range' entry is shown with a green plus icon in the Action column.

At the bottom of the settings area, there are three buttons: OK, Apply, and Cancel.

| | |
|-------------------|-----------------------------|
| Device Name: | br0 |
| Status: | Connected |
| Schedule: | Always ▾ |
| Network: | LAN ▾ |
| Connection Type: | Bridge |
| Physical Address: | 00 : 26 : 5a : 49 : 3e : 08 |
| MTU: | Automatic ▾ 1500 |

Device Name: Displays the name of the Interface.

Status: Displays the current connection state.

Schedule: Select a time frame from the drop-down menu to have your wired devices able to connect to the Internet.

Network: LAN is selected.

Connection Type: Displays the connection type the Gateway is set to.

Physical Address: Displays the MAC address of the Gateway (LAN side).

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.

Internet Protocol



| | | | | |
|-------------------|--------------------------------|-----|-----|---|
| Internet Protocol | Use the Following IP Address ▼ | | | |
| IP Address: | 192 | 168 | 1 | 1 |
| Subnet Mask: | 255 | 255 | 255 | 0 |

Internet Protocol: Select **Use the Following IP Address** from the drop-down menu.

IP Address: If you want to change the Gateway IP address, enter it here. If you do change this IP address, you must use it in the future to log into the Gateway.

Subnet Mask: Enter the Subnet Mask of your local network.

DNS Server

| | | | | |
|-----------------------|--|---|---|---|
| DNS Server | Use the Following DNS Server Addresses ▼ | | | |
| Primary DNS Server: | 0 | 0 | 0 | 0 |
| Secondary DNS Server: | 0 | 0 | 0 | 0 |

DNS Server: Select **Use the Following DNS Server Addresses** from the drop-down menu.

Primary DNS Server: Enter the IP Address of your primary DNS server.

Secondary DNS Server: Enter the IP Address of your secondary DNS server.

DHCP stands for Dynamic Host Control Protocol. The Gateway has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers /devices on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically." When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the Gateway. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer/device. You must specify the starting and ending address of the IP address pool (refer to the next page).

| IP Address Distribution | DHCP Server ▾ |
|--|---|
| Start IP Address: | <input style="width: 40px;" type="text" value="192"/> <input style="width: 40px;" type="text" value="168"/> <input style="width: 40px;" type="text" value="1"/> <input style="width: 40px;" type="text" value="1"/> |
| End IP Address: | <input style="width: 40px;" type="text" value="192"/> <input style="width: 40px;" type="text" value="168"/> <input style="width: 40px;" type="text" value="1"/> <input style="width: 40px;" type="text" value="254"/> |
| Subnet Mask: | <input style="width: 40px;" type="text" value="255"/> <input style="width: 40px;" type="text" value="255"/> <input style="width: 40px;" type="text" value="255"/> <input style="width: 40px;" type="text" value="0"/> |
| WINS Server: | <input style="width: 40px;" type="text" value="0"/> <input style="width: 40px;" type="text" value="0"/> <input style="width: 40px;" type="text" value="0"/> <input style="width: 40px;" type="text" value="0"/> |
| Lease Time in Minutes: | <input style="width: 60px;" type="text" value="60"/> |
| <input checked="" type="checkbox"/> Provide Host Name If Not Specified by Client | |
| <input checked="" type="checkbox"/> Provide DNS Server to Clients | |

DNS Server: Select **DHCP Server** from the drop-down menu (default setting) if you want the Gateway to automatically assign your wired and wireless clients their network settings automatically. If you disable this function, you will have to statically assign the IP/network settings on your clients.

Start IP Address: Enter the starting IP address of the DHCP range.

End IP Address: Enter the end IP address of the DHCP range.

Subnet Mask: Enter the subnet mask of your local network.

WINS Server: Enter the IP address of your WINS server (if one).

Lease Time in Minutes: Enter the DHCP lease time (in minutes).

Provide Host Name if Not Specified by Client: If the DHCP client does not have a host name, the Gateway will automatically assign one.

Provide DNS Server to Clients: Check this box if you want the Gateway to assign your clients the IP address(es) of the ISPs DNS servers.

DHCP Server Pools (DHCP Reservation)



If you want a computer or device to always have the same IP address assigned, you can create a DHCP reservation. The router will assign the IP address only to that computer or device.

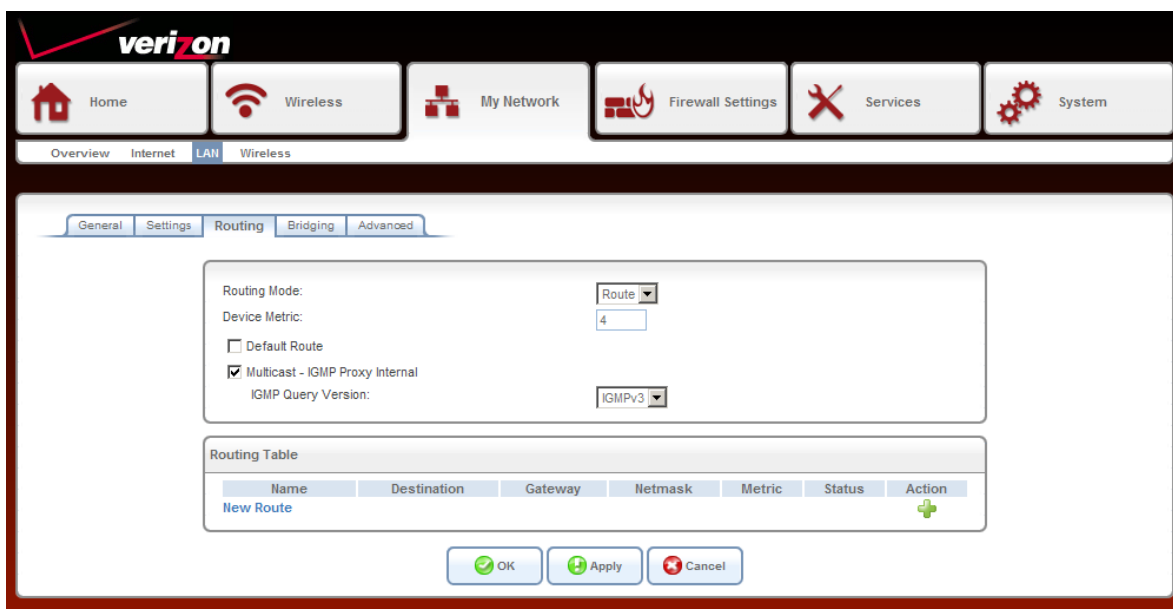
| DHCP Server Pools | | |
|------------------------------|------------------|--------|
| Criteria | Dynamic IP Range | Action |
| New IP Range | | |

Criteria: Displays the current created server pool.

Dynamic IP Range: Displays the IP address range.

Action: Click the green + sign to add a new rule, click the pencil icon to edit, or click the red X to remove the rule.

New IP Range: Click to add a new entry.



Routing Mode: Select the routing mode from the drop-down menu.

Device Metric: Enter the metric value. The route metric is a value from 1 to 15 that indicates the cost of using this route. A value 1 is the lowest cost and 15 is the highest cost.

Default Route: Check this box to use the default route.

Multicast - IGMP Proxy Internal: This box is checked by default.

IGMP Query Version: Select the IGMP Query version from the drop-down menu.

Routing Table: Displays the entered routes.

Name: Displays the name of the route you created.

Destination: The IP address of the destination location.

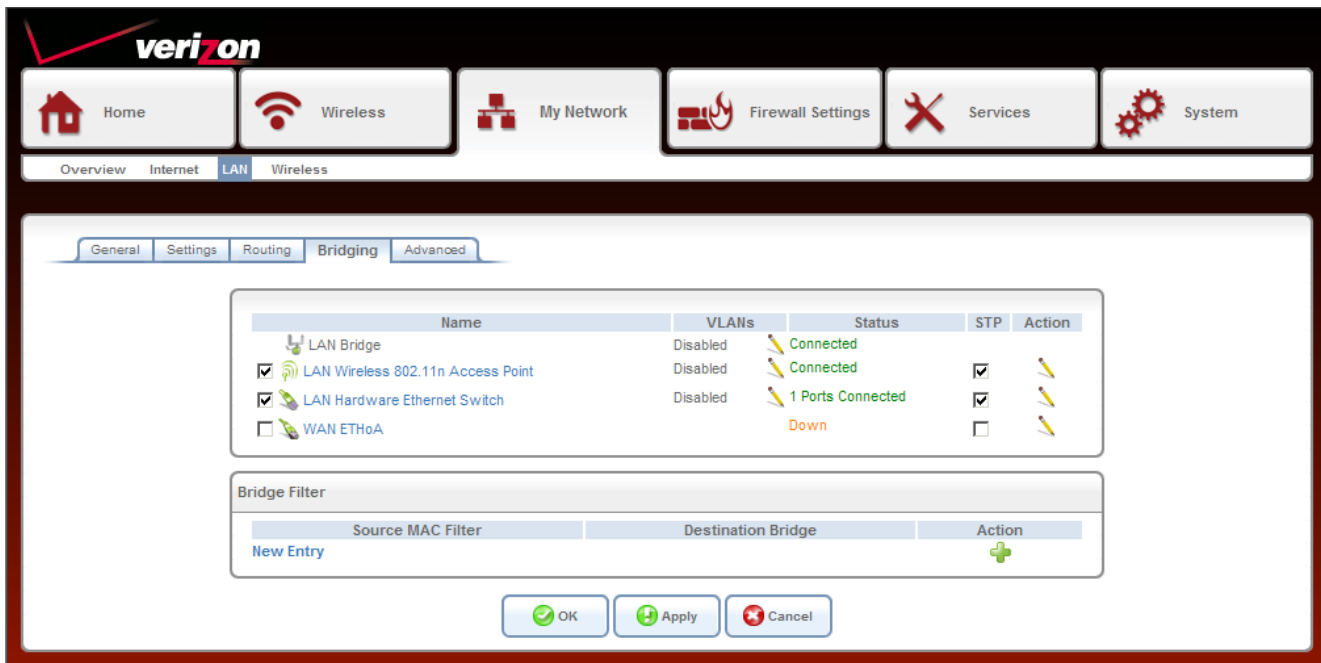
Gateway: The gateway IP address of the destination location.

Netmask: The netmask of the destination location.

Metric: The metric value assigned to this route.

Status: Displays the status of the route.

Action: Click the green + icon to add a new route, click the pencil icon to edit the route, or click the red X to delete the route.



Bridging: Displays the default segments of the Gateway. Click the pencil icon to edit the settings.

Name: The name of the segment.

VLANs: The VLAN status of the segment.

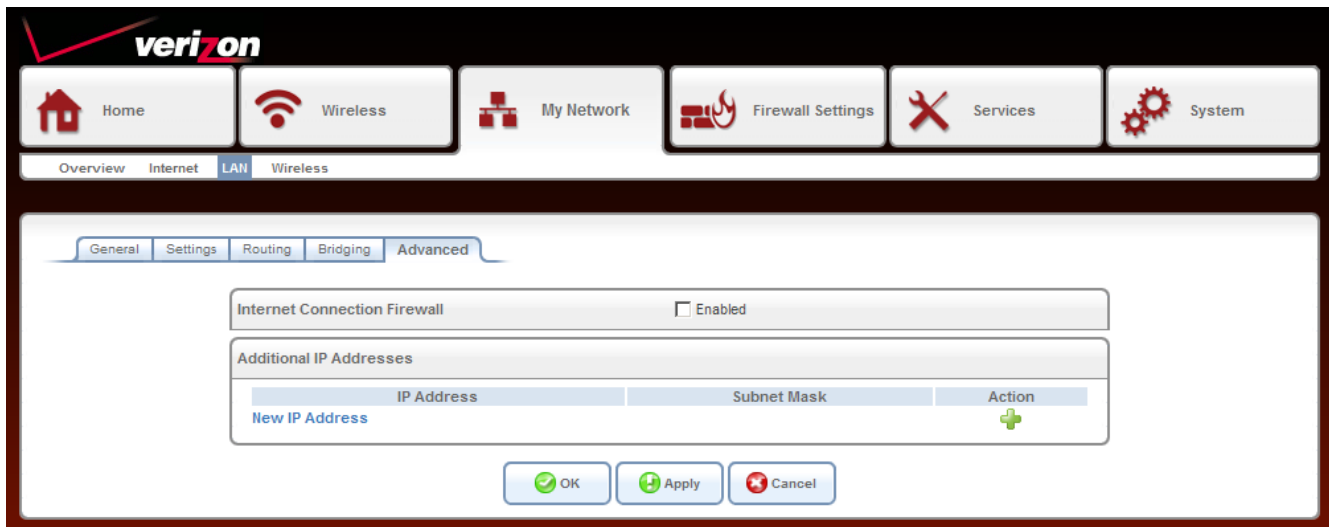
Status: The connection status of the segment.

STP: (Spanning Tree Protocol) is a method for automatically calculating the best route of a network with or without loops.

Action: Click the pencil icon to edit the segment.

Bridge Filter: You can enter your own devices to add to the bridge filter table. Click **New Entry** to add a device to the LAN Bridge.

Action: Click the green + icon to add a new entry, click the pencil icon to edit, or click the red X to delete the entry.



Internet Connection Firewall: Check the Enable box to enable the firewall feature for your wired computers/devices.

New IP Address: Click to add a new device.

IP Address: The IP address of the computer or device.

Subnet Mask: The subnet mask of the computer or device.

Action: Click the green + sign to add a computer or device, or click the red X to delete the computer or device.

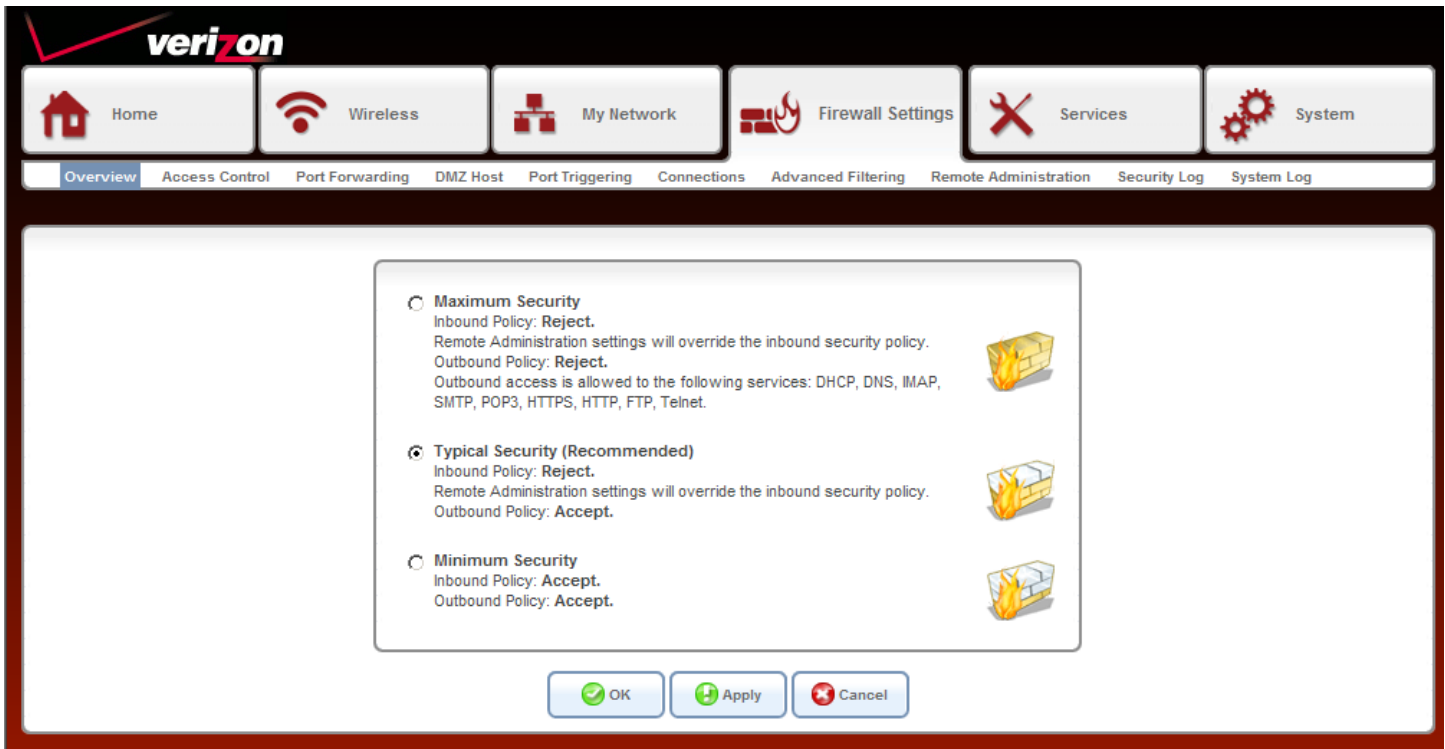
Firewall Settings

Overview



This section explains how to configure your Router's firewall security features. The Router's firewall security settings allow you reduce the risk of unauthorized access to your network by prohibiting certain types of inbound and outbound network traffic and by allowing you to configure specific firewall rules.

To change your firewall security level, click the option next to the desired security setting. Next, click **Apply** to allow the changes to take effect.



Maximum Security High security level only allows basic Internet functionality. Only Mail, News, Web, FTP, and **(High):** IPSEC are allowed. All other traffic is prohibited.

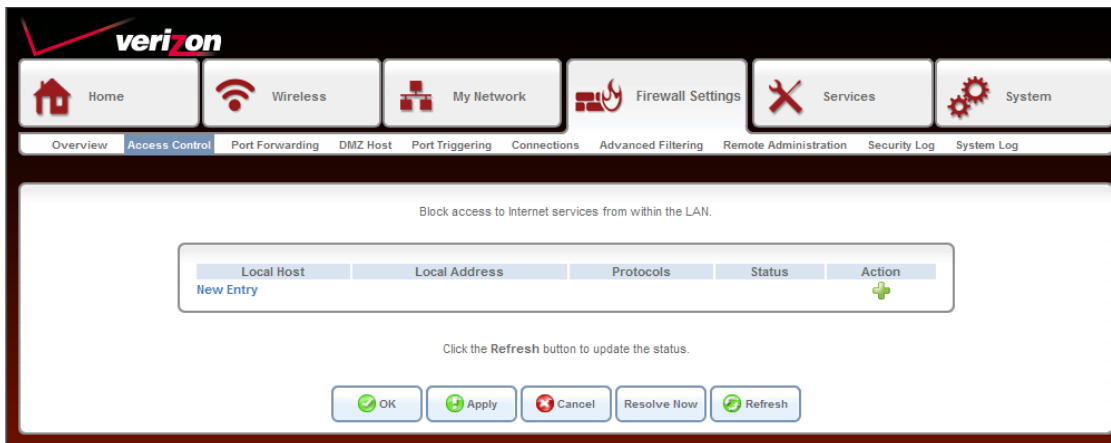
Typical Security Like High security, Medium security only allows basic Internet functionality by default. **(Medium):** However, Medium security allows customization through NAT configuration so that you can enable the traffic that you want to pass.

Minimum Security Low security setting will allow all traffic except for known attacks. With Low security, your **(Low):** Gateway is visible to other computers on the Internet.

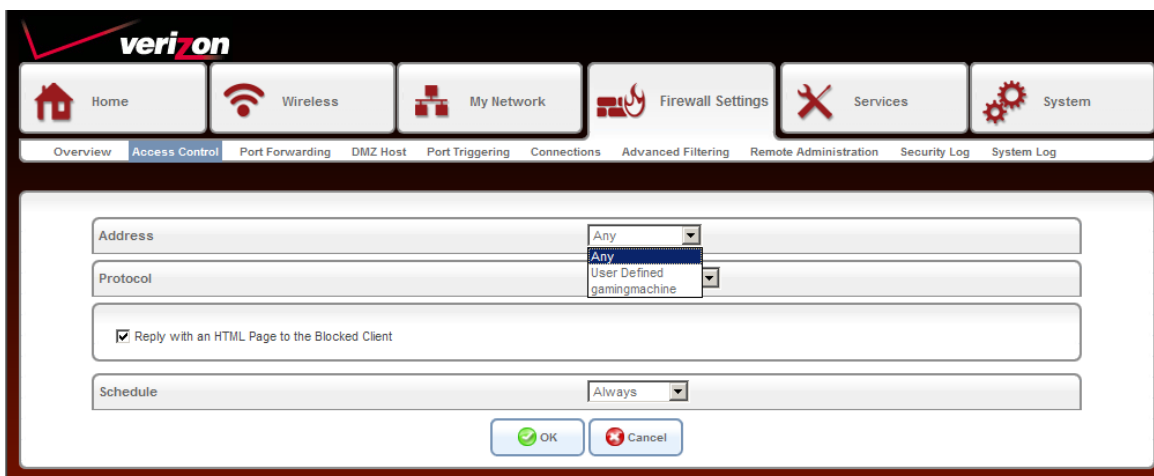
Access Control



The Access Control section allows you to control access in and out of your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications like P2P utilities or games.



Click **New Entry** to add a rule.



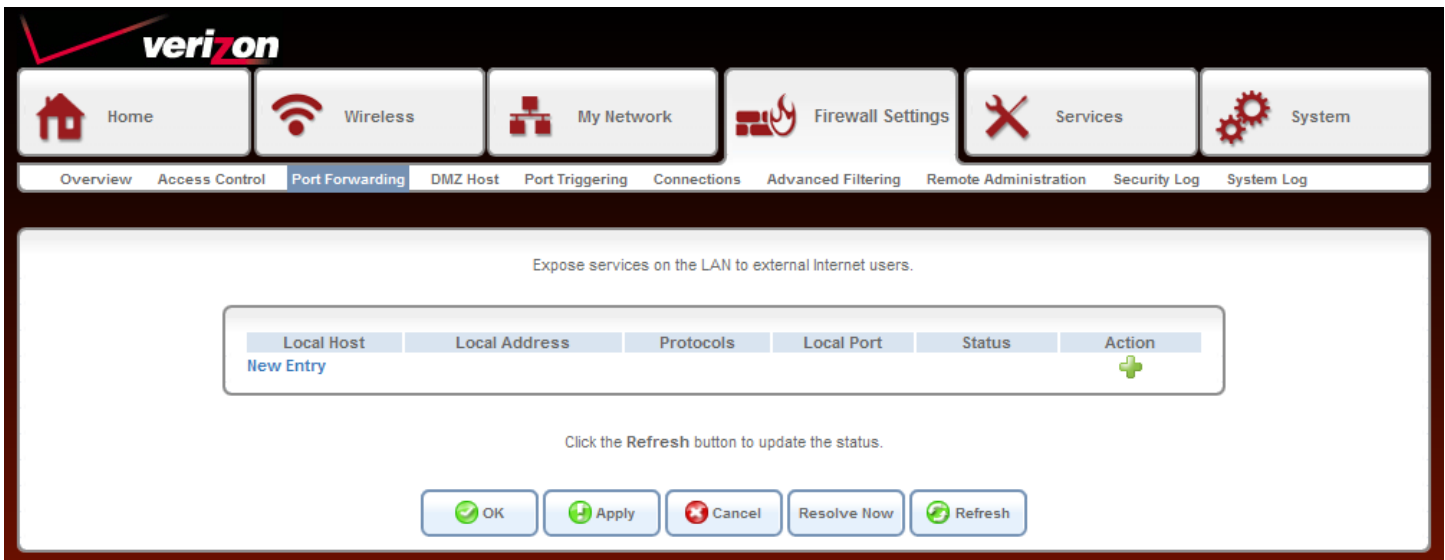
Address: Select a device from the list or select **User Defined** to create a new object.

Protocol: Select the protocol or service you want to block. The default list will have basic services. You can select **Show All Services** for a large list. If you do not see the service you want, select **User Defined** to create your own. The complete list can be view and edited at **System > Objects and Rules > Protocols**.

Reply with an HTML Page: Check this box if you want to redirect the user who tries to access a blocked service to a website of your choice. To change the web site, go to **Services > Parental Control > Advanced Options**.

Schedule: Select **Any** or a user defined schedule. Select **User Defined** to create a schedule rule. You can create/view/edit schedules at **Services > Objects and Rules > Scheduler Rules**.

Port Forwarding allows you to open a single port or a range of ports. Certain applications and games may require ports to be opened or forwarded to your computer to work. Click **New Entry** to create a rule.



Local Host: Displays the name of the host name.

Local Address: Displays the IP address of the host.

Protocols: Displays the protocol(s) used in the port forwarding rule.

Local Port: Displays the port(s) used in the port forwarding rule.

Status: Displays the current status of the rule (Active or Disabled).

Action: Click the green + icon to add a new entry, click the pencil icon to edit, or click the red X to delete the entry.

New Entry: Click to add a new port forwarding rule (refer to the next page).

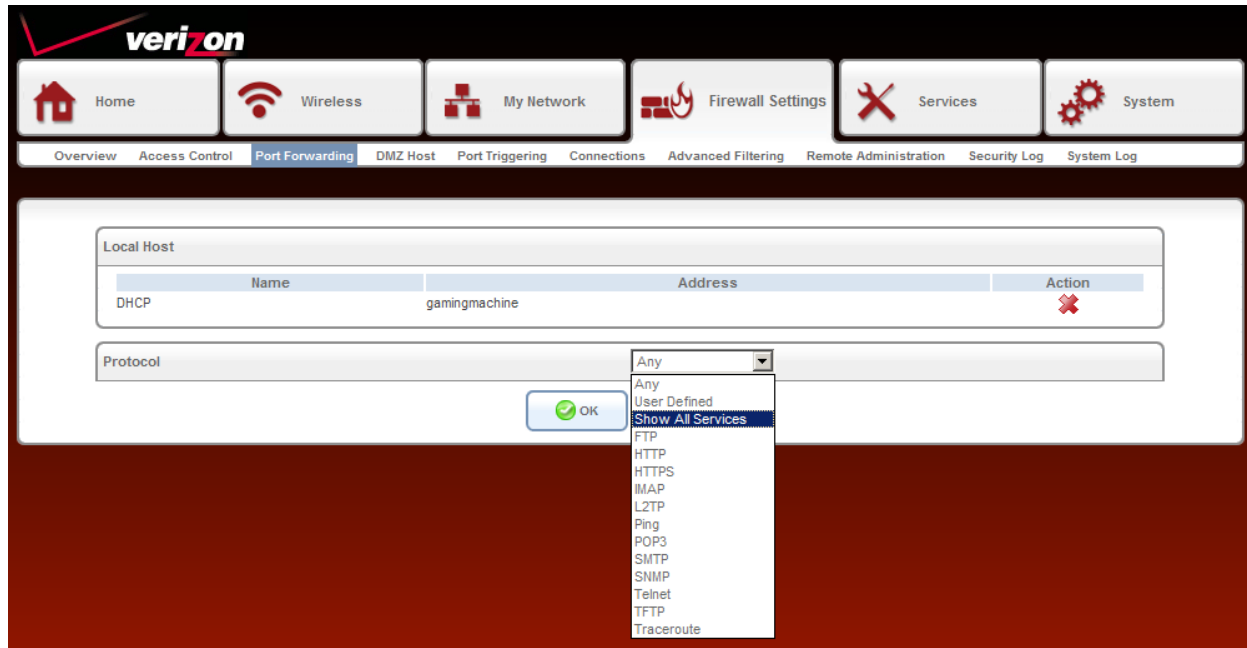
Create a Rule



Step 1: Click New Entry.

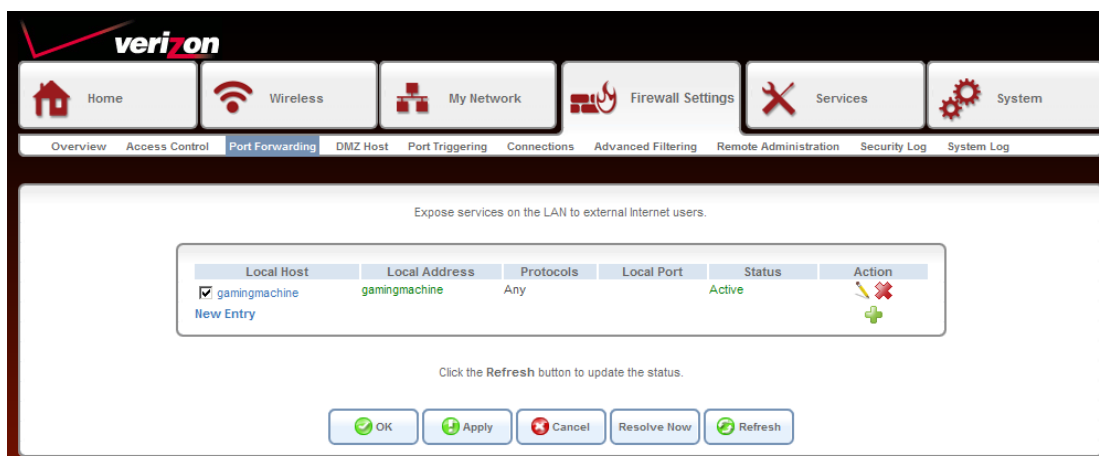
Step 2: Next to Local Host, select a computer or device from the drop-down menu.

Step 3: Next to Protocols, select a pre-defined service from the drop-down menu. The default list will have basic services. Select **Show All Services** for a much larger list of specific games and applications. If you do not see the service you want, select **User Defined** to create your own. The complete list can be view and edited at **System > Objects and Rules > Protocols**.



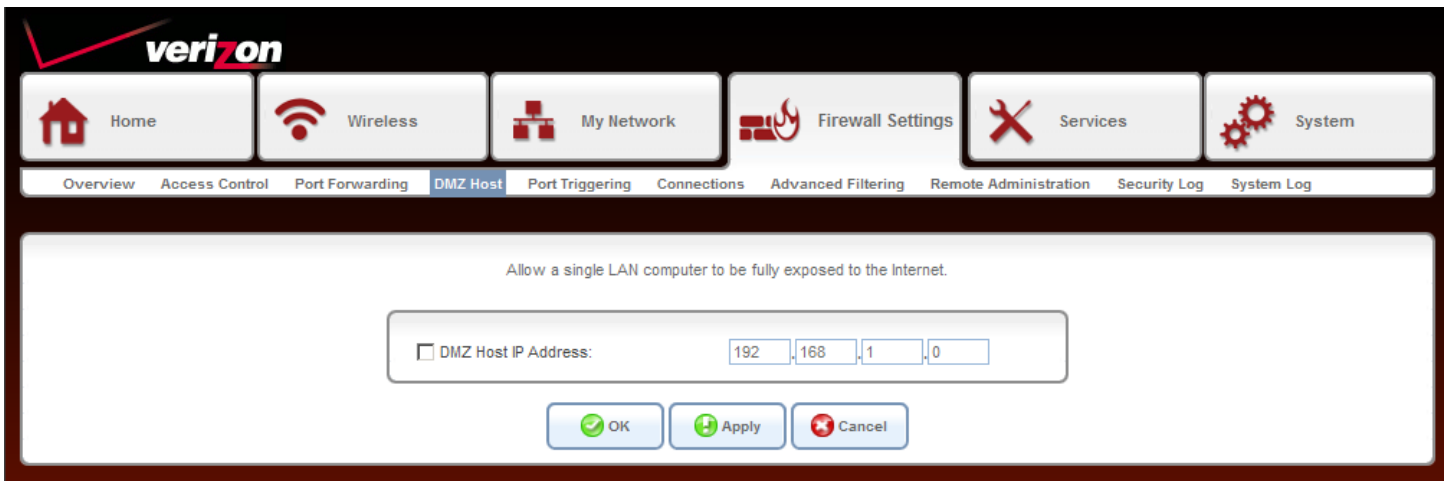
Step 4: Click **OK** to save the rule.

Step 5: The new rule will appear in the list. You can click the green + icon to add a new entry, click the pencil icon to edit, or click the red X to delete the entry.



If an application has trouble working from behind the Gateway, you can expose one computer to the Internet and run the application on that computer.

Note: Placing a computer in the DMZ will expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.



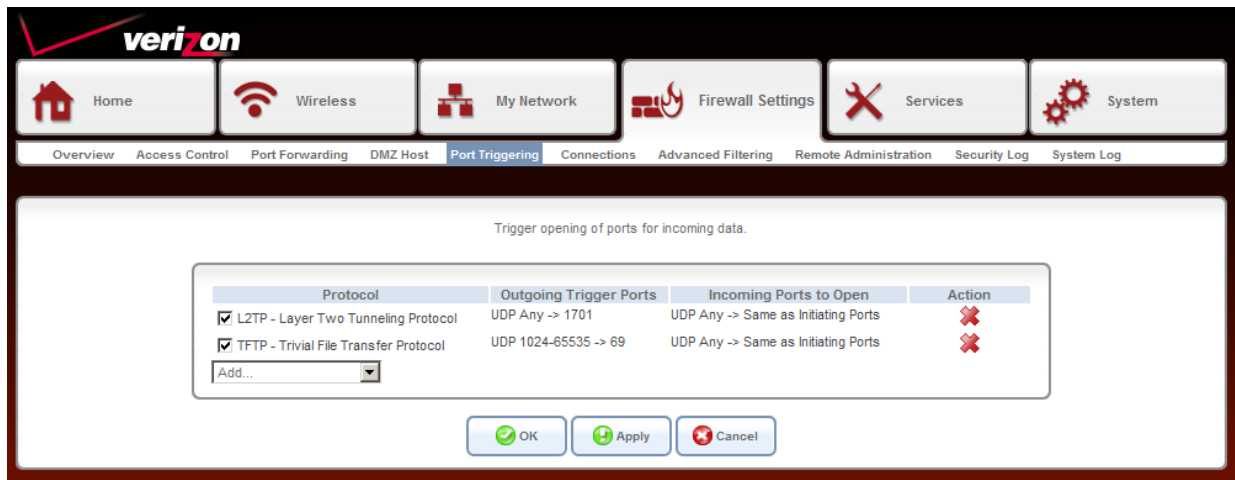
The screenshot shows the Verizon DSL-2750B web interface. At the top, there is a navigation bar with icons and labels for Home, Wireless, My Network, Firewall Settings, Services, and System. Below this is a secondary navigation bar with links for Overview, Access Control, Port Forwarding, DMZ Host (which is highlighted), Port Triggering, Connections, Advanced Filtering, Remote Administration, Security Log, and System Log. The main content area displays the text "Allow a single LAN computer to be fully exposed to the Internet." Below this text is a form with a checkbox labeled "DMZ Host IP Address:" and four input fields containing the IP address "192.168.1.0". At the bottom of the form are three buttons: "OK", "Apply", and "Cancel".

DMZ Host IP Address: Check the box to DMZ. This will de-activate any port-forwarding rules.

Enter the IP address of the computer you want to open to the Internet.

The Port Triggering feature allows you to forward a range of ports to an IP address on your local network (LAN) only after specific outbound traffic is detected. You can set up a port triggering entry based on your specific ports.

IMPORTANT: Using various Internet applications depends on the Router's firewall settings. Make sure that the Router's firewall is set to Medium Security or lower to take advantage of all the port forwarding features. Firewall settings take precedence over port forwarding services configured in the Router. For example, if the firewall is set to Medium Security, this will block ICMP packets even if the ICMP service is enabled. If a port forwarding service is not working, try setting the firewall to a lower setting.



Protocol: Displays the protocol/service. Check the box to activate the rule.

Outgoing Trigger Ports: Displays the outgoing port(s) and protocol(s) used by the application.

Incoming Ports to Open: Displays the incoming port(s) and protocol(s) opened by the application.

Action: Click the red X to delete the rule.

Add: Select a service/application from the drop-down menu to add.

Connections



This page will display connection from your local network (LAN) to the Internet.

verizon

Home Wireless My Network Firewall Settings Services System

Overview Access Control Port Forwarding DMZ Host Port Triggering **Connections** Advanced Filtering Remote Administration Security Log System Log

Active Connections: 0
Approximate Max. Connections: 149

Connection List

| Number | Protocol | LAN IP:Port | Verizon IP:Port | WAN IP:Port | Direction | Action |
|--------|----------|-------------|-----------------|-------------|-----------|--------|
|--------|----------|-------------|-----------------|-------------|-----------|--------|

Click the Refresh button to update the status.

Close Refresh Advanced >>

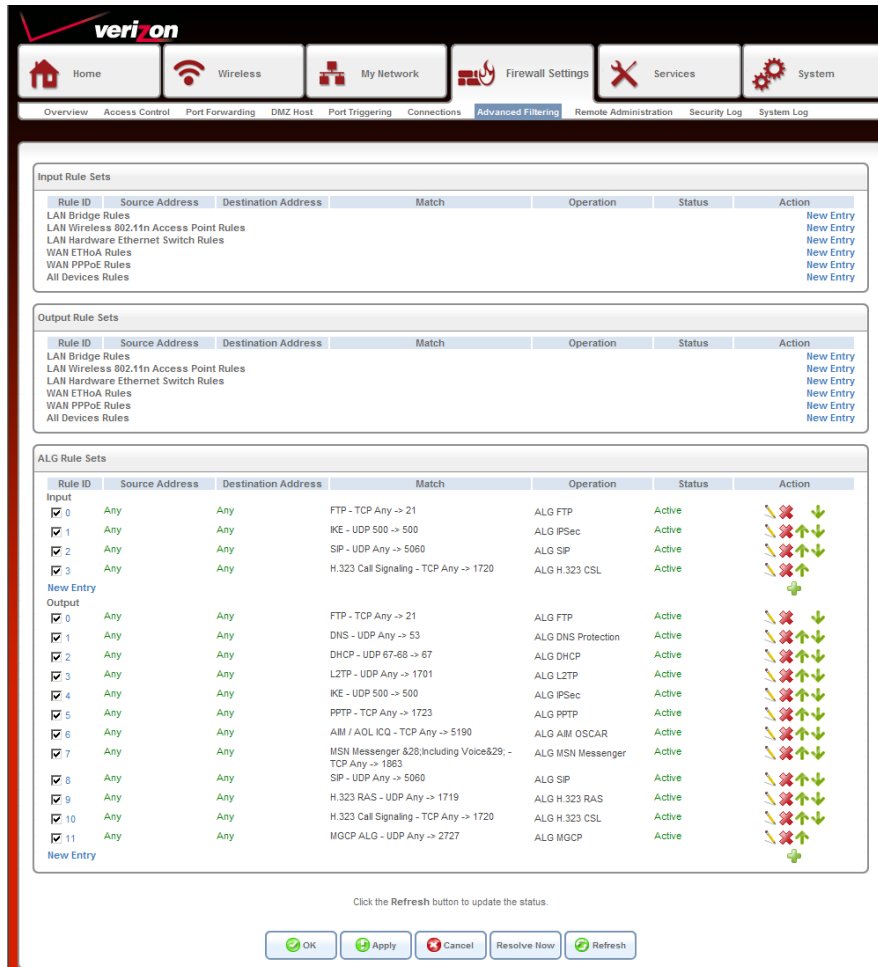
Action: Click the red X to delete the listing.

Close: Click to go to the Overview page.

Advanced Filtering



Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). Port Triggering makes some of these applications work with the Gateway.



Protocol: Displays the protocol/service. Check the box to activate the rule.

Outgoing Trigger Ports: Displays the outgoing port(s) and protocol(s) used by the application.

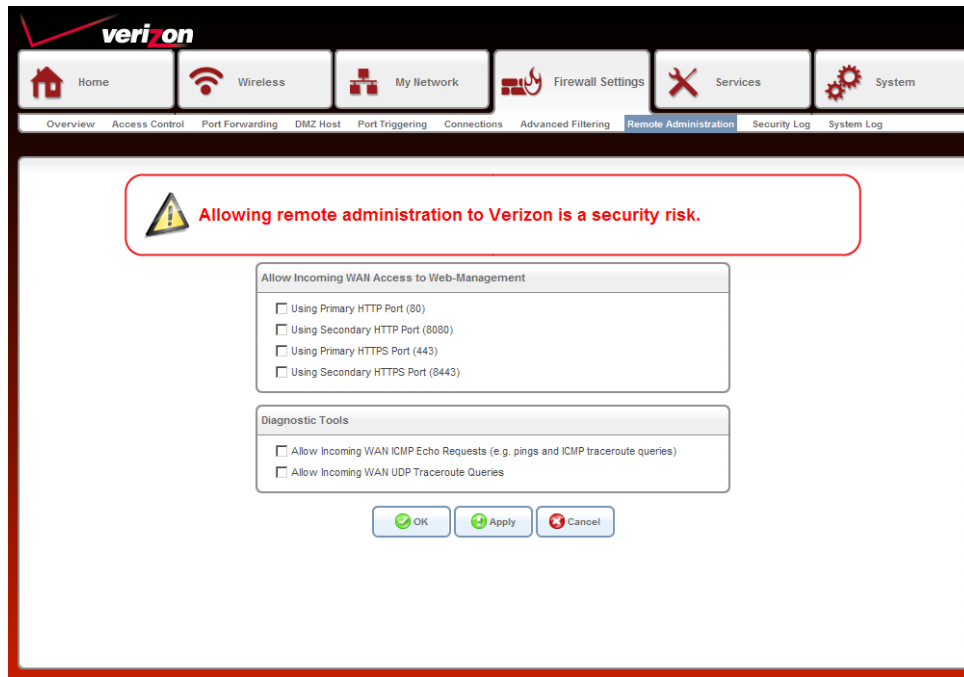
Incoming Ports to Open: Displays the incoming port(s) and protocol(s) opened by the application.

Action: Click the red X to delete the rule.

Add: Select a service/application from the drop-down menu to add.

Remote management allows the Gateway to be configured from the Internet by a web browser. A username and password is still required to access the Web-Management interface.

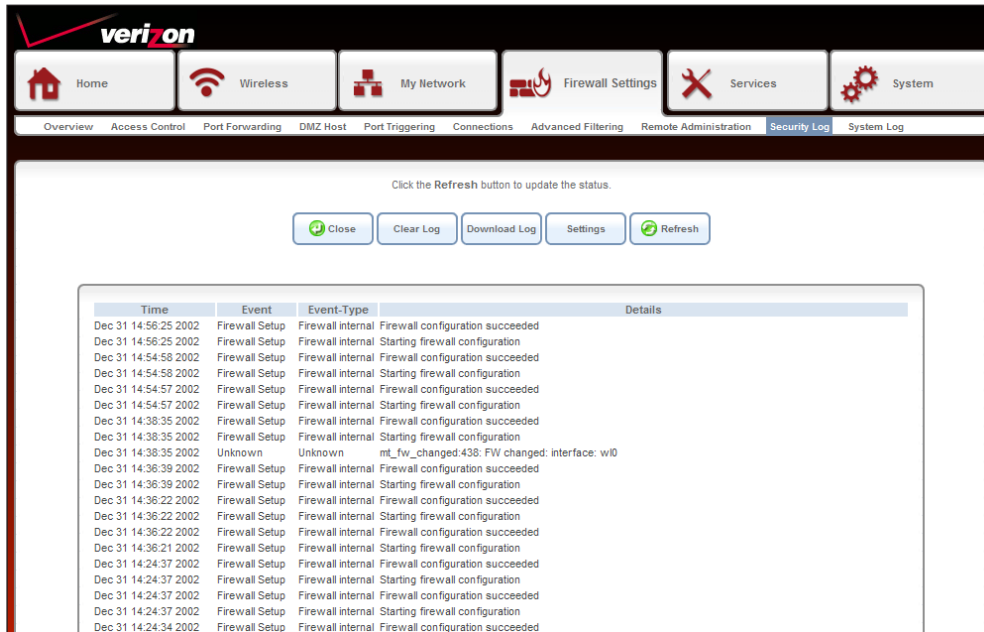
Example: `http://x.x.x.x:8080` whereas x.x.x.x is the WAN IP address of the Gateway and 8080 is the port used for the Web Management interface.



Allow Incoming WAN Access to Web Management: Check the box of the port you want to use. The default port is 80.

Diagnostic Tools: Check the box to activate the diagnostic tools rule.

The Gateway automatically logs (records) security events of possible interest in its internal memory. If there isn't enough internal memory for all events, logs of older events are deleted but logs of the latest events are retained. The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of the events to view.



Close: Click to close the log page.

Clear Log: Click to delete all the log entries.

Download Log: Click to save the log to your computer.

Settings: Click to select filters for the information displayed in the log (refer to the next page).

Refresh: Click to update the log details on the screen so it displays any recent activity.

Settings



Check the box(es) below to include in the security log.

Accepted Events

Accepted Incoming Connections

Accepted Outgoing Connections

Blocked Events

| | | |
|--|---|---|
| <input type="checkbox"/> All Blocked Connection Attempts | <input type="checkbox"/> Multicast/Broadcast | <input type="checkbox"/> ICMP Replay |
| <input type="checkbox"/> Winnuke | <input type="checkbox"/> Spoofed Connection | <input type="checkbox"/> ICMP Redirect |
| <input type="checkbox"/> Defragmentation Error | <input type="checkbox"/> Packet Illegal Options | <input type="checkbox"/> ICMP Multicast |
| <input type="checkbox"/> Blocked Fragments | <input type="checkbox"/> UDP Flood | <input type="checkbox"/> ICMP Flood |
| <input type="checkbox"/> Syn Flood | | |
| <input type="checkbox"/> Echo Chargen | | |

Other Events

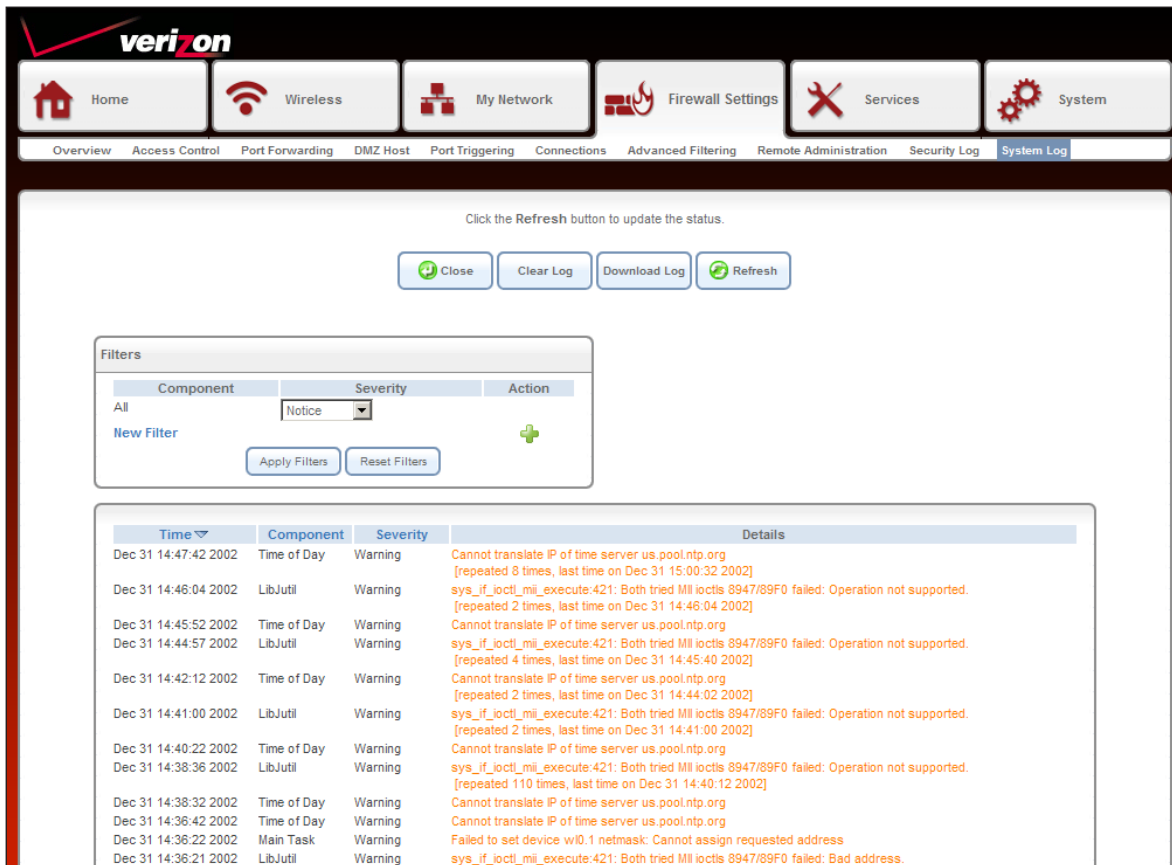
Remote Administration Attempts

Connection States

Log Buffer

Prevent Log Overrun

The Gateway automatically logs (records) system events of possible interest in its internal memory. If there isn't enough internal memory for all events, logs of older events are deleted but logs of the latest events are retained. The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of the events to view.



Click the Refresh button to update the status.

Close Clear Log Download Log Refresh

Filters

| Component | Severity | Action |
|---------------|----------|---------------|
| All | Notice | |
| New Filter | | + |
| Apply Filters | | Reset Filters |

| Time | Component | Severity | Details |
|----------------------|-------------|----------|---|
| Dec 31 14:47:42 2002 | Time of Day | Warning | Cannot translate IP of time server us.pool.ntp.org [repeated 8 times, last time on Dec 31 15:00:32 2002] |
| Dec 31 14:46:04 2002 | LibJutil | Warning | sys_if_ioctl_mi_execute:421: Both tried MI ioctl's 8947/89F0 failed: Operation not supported. [repeated 2 times, last time on Dec 31 14:46:04 2002] |
| Dec 31 14:45:52 2002 | Time of Day | Warning | Cannot translate IP of time server us.pool.ntp.org |
| Dec 31 14:44:57 2002 | LibJutil | Warning | sys_if_ioctl_mi_execute:421: Both tried MI ioctl's 8947/89F0 failed: Operation not supported. [repeated 4 times, last time on Dec 31 14:45:40 2002] |
| Dec 31 14:42:12 2002 | Time of Day | Warning | Cannot translate IP of time server us.pool.ntp.org [repeated 2 times, last time on Dec 31 14:44:02 2002] |
| Dec 31 14:41:00 2002 | LibJutil | Warning | sys_if_ioctl_mi_execute:421: Both tried MI ioctl's 8947/89F0 failed: Operation not supported. [repeated 2 times, last time on Dec 31 14:41:00 2002] |
| Dec 31 14:40:22 2002 | Time of Day | Warning | Cannot translate IP of time server us.pool.ntp.org |
| Dec 31 14:38:36 2002 | LibJutil | Warning | sys_if_ioctl_mi_execute:421: Both tried MI ioctl's 8947/89F0 failed: Operation not supported. [repeated 110 times, last time on Dec 31 14:40:12 2002] |
| Dec 31 14:38:32 2002 | Time of Day | Warning | Cannot translate IP of time server us.pool.ntp.org |
| Dec 31 14:36:42 2002 | Time of Day | Warning | Cannot translate IP of time server us.pool.ntp.org |
| Dec 31 14:36:22 2002 | Main Task | Warning | Failed to set device w0.1 netmask: Cannot assign requested address |
| Dec 31 14:36:21 2002 | LibJutil | Warning | sys_if_ioctl_mi_execute:421: Both tried MI ioctl's 8947/89F0 failed: Bad address. |

Close: Click to close the log page and go back to the Overview page.

Clear Log: Click to delete all the log entries.

Download Log: Click to save the log to your computer.

Refresh: Click to update the log details on the screen so it displays any recent activity.

Filters: Select specific items to record in the log or click **New Filter** to add an item. Click **Apply Filters** to add it to the list.

Services Overview

This page displays the status of each service. Click on the service to configure.

Services

- QoS: Default
- Storage: No Disks Online
- IP Address Distribution: Enabled
- Parental Control: Disabled
- Personal Domain Name: Disabled

Click the Refresh button to update the status.

Close Refresh

QoS Overview



This screen allows you to configure Quality of Service parameters in the Gateway. Select the profile that fits you the best and click **OK**.

WAN Devices Bandwidth (Rx/Tx): Automatic

QoS Profiles

Default
No Quality of Service preferences

P2P User
"I use peer-to-peer and file-sharing applications. I still want to be able to use my browser without interference."

HTTP/HTTPS: **Medium**
TCP ACKs: **Medium**
Other: **Low**

Triple Play User
"I use VoIP applications and video streaming. I want these applications to be as fast as possible."

VoIP (SIP, H323): **High**
Video: **High-Medium**
HTTP/HTTPS: **Medium**
Other: **Low**

Home Worker
"I work from home, and want my VPN and browser to have priority over other traffic."

VPN (IPsec, L2TP, PPTP): **Medium**
HTTP/HTTPS: **Medium**
Other: **Low**

Gamer
"I play games over the Internet and want the games-related traffic to be as fast as possible."

Games Related Traffic: **Medium**
Other: **Low**

Priority By Host
"I want to give different hosts in my network different priorities when accessing the public network."

High Priority Host:
Low Priority Host:
Other: **Medium**

Note: Selecting a new QoS profile will cause all previous configuration settings to be lost

Utilization by Computer



This screen displays bandwidth usage from computers on your local network.

The screenshot shows the Verizon DSL-2750B web interface. At the top, there is a navigation bar with the Verizon logo and several menu items: Home, Wireless, My Network, Firewall Settings, Services, and System. Below this is a sub-navigation bar with options: Overview, QoS, Parental Control, Storage, Personal Domain Name, IP Address Distribution, and Advanced. The main content area is titled "Utilization by Computer" and includes a sub-menu: Overview, Utilization by Computer, Utilization by Application, Traffic Priority, Traffic Shaping, DSCP Settings, 802.1p Settings, and Class Statistics. The page text states: "This page provides your Internet connection's bandwidth usage information at the computer level." Below this is a table header with columns: Computer, Tx Throughput (Kbps), and Rx Throughput (Kbps). A note says "Click the Refresh button to update the status." At the bottom are three buttons: Close, Automatic Refresh Off, and Refresh.

Utilization by Application

This screen displays bandwidth usage from applications on your local network.

The screenshot shows the Verizon DSL-2750B web interface. At the top, there is a navigation bar with the Verizon logo and several menu items: Home, Wireless, My Network, Firewall Settings, Services, and System. Below this is a sub-navigation bar with options: Overview, QoS, Parental Control, Storage, Personal Domain Name, IP Address Distribution, and Advanced. The main content area is titled "Utilization by Application" and includes a sub-menu: Overview, Utilization by Computer, Utilization by Application, Traffic Priority, Traffic Shaping, DSCP Settings, 802.1p Settings, and Class Statistics. The page text states: "This page provides your Internet connection's bandwidth usage information at the application level." Below this is a table header with columns: Application, Protocol, Port, Tx Throughput (Kbps), and Rx Throughput (Kbps). A link below the Application column says "Click here to add a new Application definition". A note says "Click the Refresh button to update the status." At the bottom are three buttons: Close, Automatic Refresh Off, and Refresh.

Traffic Priority



This screen displays the QoS input and output rules. These will change depending on the selection you selected on the **Services > QoS > Overview** page.

The screenshot shows the Verizon DSL-2750B web interface. At the top, there is a navigation bar with icons for Home, Wireless, My Network, Firewall Settings, Services, and System. Below this is a sub-menu with options: Overview, QoS, Parental Control, Storage, Personal Domain Name, IP Address Distribution, and Advanced. The main content area is titled 'Traffic Priority' and contains two sections: 'QoS Input Rules' and 'QoS Output Rules'. Each section contains a table with columns for Rule ID, Source Address, Destination Address, Match, Operation, Status, and Action. The 'QoS Input Rules' table shows two active rules: Rule 7 (SIP - UDP 5060 -> Any) and Rule 8 (IGMP - Protocol 2). The 'QoS Output Rules' table shows two active rules: Rule 0 (SIP - UDP Any -> 5060) and Rule 1 (IGMP - Protocol 2). The interface also includes a 'Done' button at the bottom left and a system tray at the bottom right showing 'Internet' and '100%' zoom.

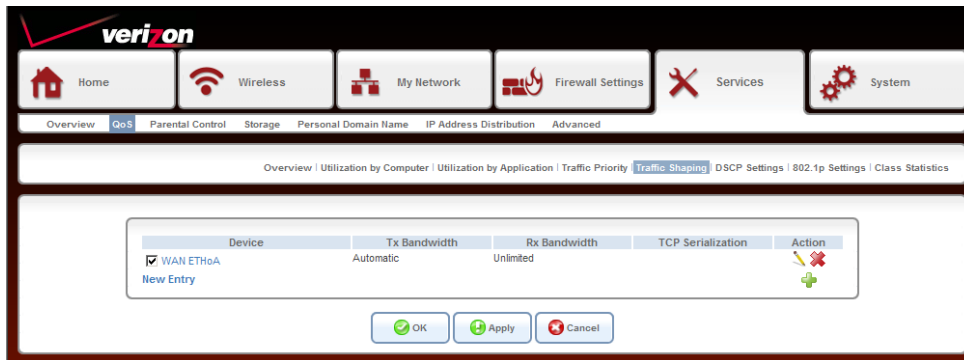
| Rule ID | Source Address | Destination Address | Match | Operation | Status | Action |
|-------------|----------------|---------------------|-----------------------|--|--------|------------------------------|
| 7 | Any | Any | SIP - UDP 5060 -> Any | Priority 7 (Queue 3 - Highest) DSCP 0X2E Mask 0X3F | Active | [Edit] [Delete] [Down Arrow] |
| 8 | Any | Any | IGMP - Protocol 2 | Priority 6 (Queue 3 - Highest) DSCP 0X26 Mask 0X3F No Connection | Active | [Edit] [Delete] [Up Arrow] |
| New Entry | | | | | | [Add] |
| All Devices | | | | | | |

| Rule ID | Source Address | Destination Address | Match | Operation | Status | Action |
|-----------|----------------|---------------------|-----------------------|--|--------|---|
| 0 | Any | Any | SIP - UDP Any -> 5060 | Priority 7 (Queue 3 - Highest) DSCP 0X2E Mask 0X3F | Active | [Edit] [Delete] [Down Arrow] |
| 1 | Any | Any | IGMP - Protocol 2 | Priority 6 (Queue 3 - Highest) DSCP 0X26 Mask 0X3F No Connection | Active | [Edit] [Delete] [Up Arrow] [Down Arrow] |
| New Entry | | | | | | [Add] |

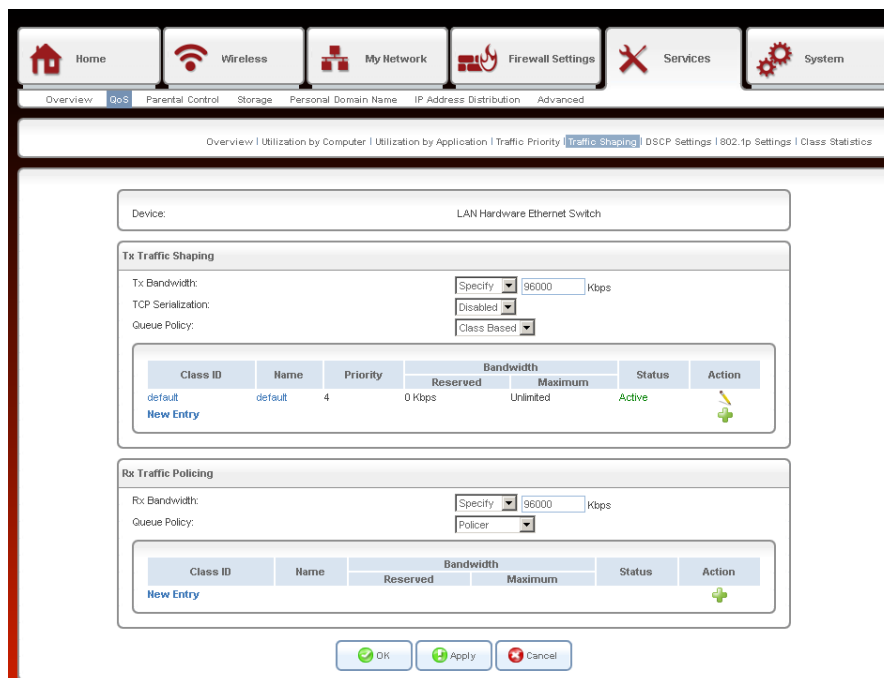
Traffic Shaping



This page allows you to add traffic shaping rules. Click **New Entry** to add a rule.



Once you click New Entry, select the device/Gateway segment you want to configure from the drop-down menu.



Tx Bandwidth: Select the Tx traffic bandwidth from the drop-down. Select **Specify** to enter your own value, **Automatic**, or **Unlimited**.

TCP Serialization: Select **Enabled** or **Disabled**.

Queue Policy: Select **Class Based** or **Strict Priority**.

Rx Bandwidth: Select the Rx traffic bandwidth from the drop-down. Select **Specify** to enter your own value, **Automatic**, or **Unlimited**.

Queue Policy: Select **Policer**, **Class Based** or **Strict Priority**.

DSCP Settings



This page allows you to configure DSCP (Differentiated Services Code Point) settings. Click the pencil icon to edit the priority and settings for each DSCP value.

| DSCP Value (hex) | 802.1p Priority | Action |
|------------------|-----------------------|--------|
| 0x0 | 0 (Queue 1 - Low) | |
| 0x2 | 0 (Queue 1 - Low) | |
| 0x4 | 4 (Queue 2 - High) | |
| 0x6 | 4 (Queue 2 - High) | |
| 0x8 | 2 (Queue 0 - Lowest) | |
| 0xA | 1 (Queue 0 - Lowest) | |
| 0xC | 3 (Queue 1 - Low) | |
| 0xE | 2 (Queue 0 - Lowest) | |
| 0x10 | 7 (Queue 3 - Highest) | |
| 0x12 | 6 (Queue 3 - Highest) | |
| 0x14 | 7 (Queue 3 - Highest) | |
| 0x16 | 6 (Queue 3 - Highest) | |
| 0x18 | 5 (Queue 2 - High) | |
| 0x1A | 5 (Queue 2 - High) | |
| 0x1C | 5 (Queue 2 - High) | |
| 0x1E | 5 (Queue 2 - High) | |
| 0x26 | 5 (Queue 2 - High) | |
| 0x2E | 7 (Queue 3 - Highest) | |

[New Entry](#)

802.1p Settings



This page allows you to configure 802.1p settings. Select the queue for each 802.1p value.

| 802.1p Value | Queue |
|--------------|-------------------|
| 0 | Queue 1 - Low |
| 1 | Queue 0 - Lowest |
| 2 | Queue 0 - Lowest |
| 3 | Queue 1 - Low |
| 4 | Queue 2 - High |
| 5 | Queue 2 - High |
| 6 | Queue 3 - Highest |
| 7 | Queue 3 - Highest |

OK Apply Cancel

Class Statistics

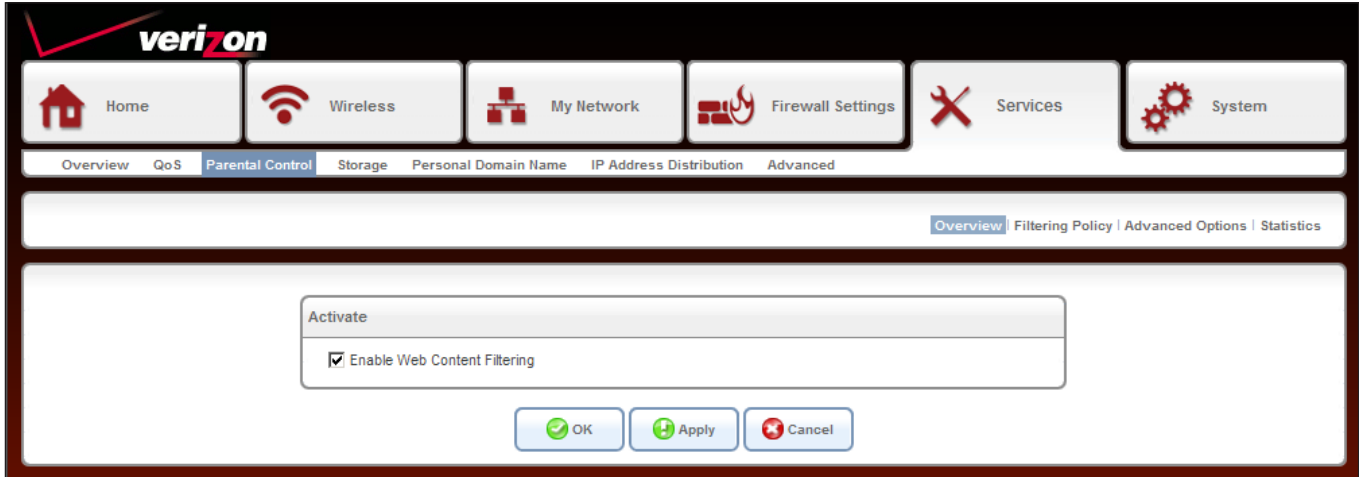


The screenshot shows the Verizon DSL-2750B web interface. At the top, there is a navigation bar with the Verizon logo and several menu items: Home, Wireless, My Network, Firewall Settings, Services, and System. Below this is a sub-menu with options: Overview, QoS, Parental Control, Storage, Personal Domain Name, IP Address Distribution, and Advanced. The main content area shows a breadcrumb trail: Overview | Utilization by Computer | Utilization by Application | Traffic Priority | Traffic Shaping | DSCP Settings | 802.1p Settings | Class Statistics. A central message box states "No statistics available". Below this message, it says "Click the Refresh button to update the status." At the bottom of the message box, there are three buttons: "Close", "Automatic Refresh Off", and "Refresh".

Parental Controls Overview



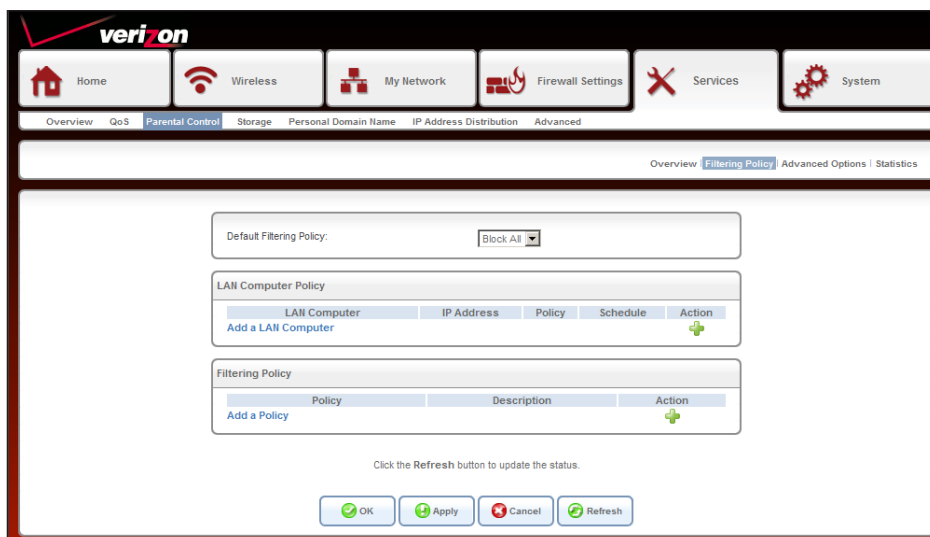
To activate parental control, check the **Enable Web Content Filtering** box and then click **OK**. You will be directed to the Filtering Policy page (refer to the next page).



Filtering Policy



Once you enable Parental Controls, you can create filtering rules here.



Default Filtering Policy: This is a global setting. If you select **Block All**, it will over-ride LAN Computer Policies and Filtering Policies created and block all computers/devices from connecting to the Internet. To use created policies, select **Allow All**.

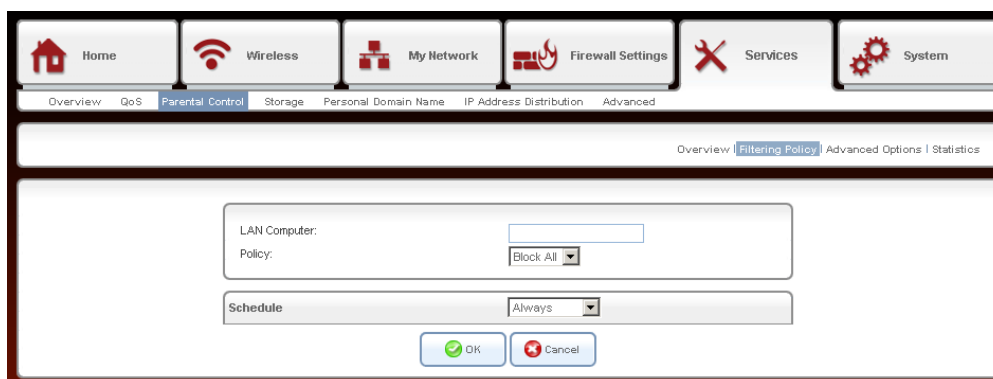
LAN Computer Policy: This list will display any LAN computer policies. You can click the green + icon to add a new entry, click the pencil icon to edit, or click the red X to delete the entry.

Click **Add a LAN Computer** to create a new entry (see below).

Filtering Policy: This list will display any filter policies that were created. You can click the green + icon to add a new entry, click the pencil icon to edit, or click the red X to delete the entry.

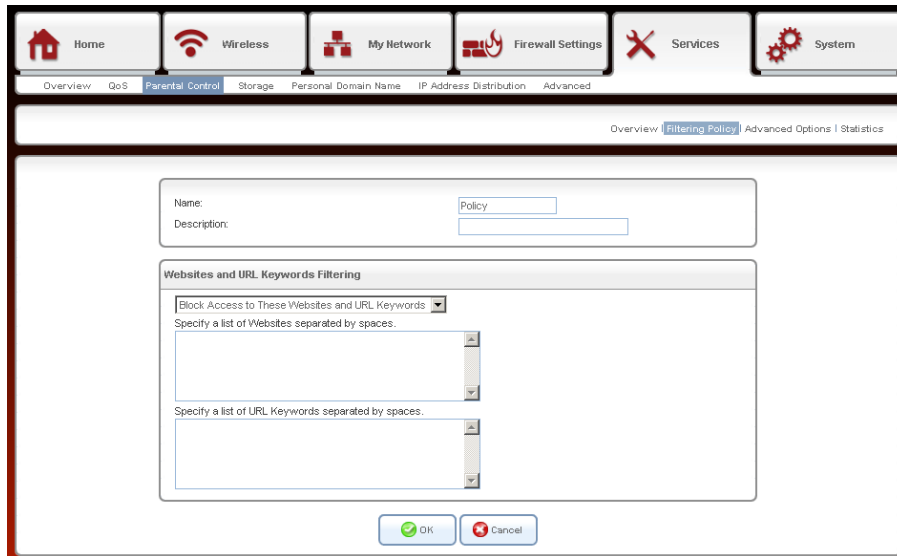
Click **Add a Policy** to create a new entry (refer to the next page).

Add a LAN Computer



Enter the name or IP address (x.x.x.x) of your computer or device and then select **Allow All**, **Block All**, or any created policy (see next page). You can then select a schedule from the drop-down. Click **OK** to continue.

WARNING: If you enter the computer you are working on and select Block All, you will disconnect from the Gateway and will not be able to log back in (since you are blocked). You will have to connect to the Gateway from another computer or reset the Gateway back to factory default settings.



Name: Enter a name for your policy.

Description: Enter a description.

Websites and URL Keywords Filtering: Select either **Block Access to These Websites and URL Keywords** or **Allow Access to These Websites and URL Keywords** from the drop-down menu.

List of Websites: Enter specific websites you want to block or allow.

List of Keywords: Enter keywords that are on websites that you want to block or allow.

OK: Click to save your policies.

Created policies will then appear in the drop-down list when adding LAN computers.

Advanced Options



If a user from your local network attempts to visit a site that you blocked, they will get redirected to the URL you want. Enter the URL below and click **OK**. Click **Reset Redirect URL** to clear out the URL.

The screenshot shows the Verizon DSL-2750B web interface. At the top, there is a navigation bar with icons for Home, Wireless, My Network, Firewall Settings, Services, and System. Below this is a secondary navigation bar with links for Overview, QoS, Parental Control, Storage, Personal Domain Name, IP Address Distribution, and Advanced. The main content area displays the 'Advanced Options' dialog box, which contains a 'Redirect URL:' label and an empty text input field. Below the input field are four buttons: 'OK' (with a green checkmark), 'Apply' (with a green plus sign), 'Cancel' (with a red X), and 'Reset Redirect URL'.

Statistics



This page displays the number of allowed and blocked sites that were attempted to be view from your local network.

The screenshot shows the Verizon DSL-2750B web interface. At the top, there is a navigation bar with the Verizon logo and several menu items: Home, Wireless, My Network, Firewall Settings, Services, and System. Below this is a sub-menu with items like Overview, QoS, Parental Control, Storage, Personal Domain Name, IP Address Distribution, and Advanced. The main content area is titled 'Statistics' and contains a table with the following data:

| Statistics | |
|------------------|--------|
| Access attempts: | 0 |
| Allowed: | 0.00 % |
| Blocked: | 0.00 % |

Below the table, there is a message: "Click the Refresh button to update the status." At the bottom of the statistics area, there are four buttons: Close, Reset Statistics, Automatic Refresh Off, and Refresh.

Storage File Server



You can connect a USB thumb drive or external hard drive to the router and share it with users on your local network.

The screenshot shows the Verizon DSL-2750B router's web interface. The top navigation bar includes Home, Wireless, My Network, Firewall Settings, Services, and System. The main content area is titled 'File Server' and contains the following sections:

- Enabled:** A checkbox labeled 'Enabled' is checked. Below it is a text field for 'NetBIOS Workgroup' containing the value 'HOME'.
- Automatic Sharing:** A checkbox labeled 'Automatically Share All Partitions' is checked. Below it is a dropdown menu for 'Allow Guest Access' set to 'Read/Write'.
- File Server Shares:** A table with columns for Name, Path, Comment, and Action. A 'New Entry' button with a plus icon is located at the bottom right of the table.

At the bottom of the page, there are four buttons: OK, Apply, Cancel, and Refresh. A note above the buttons says 'Click the Refresh button to update the status.'

Enabled: Check to enable access to your USB drive.

NetBIOS Workgroup: Enter the name of your workgroup.

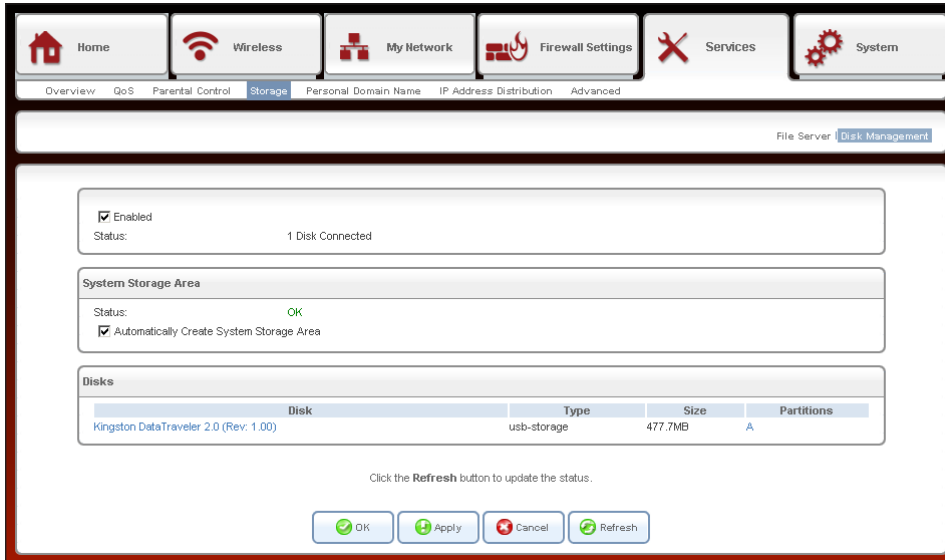
Automatically Share All Partitions: Check to automatically allow all partitions on your drive shared.

Allow Guest Access: Select the user rights for Guests - **Disabled**, **Read only**, or **Read/Write**.

File Server Shares: Your drive will appear here. Click the name of the drive to access the folders and files. Advanced users can click **New Entry** to assign specific users, groups to specific folders on your USB drive.

OK: Click **OK** to save your settings.

Disk Management



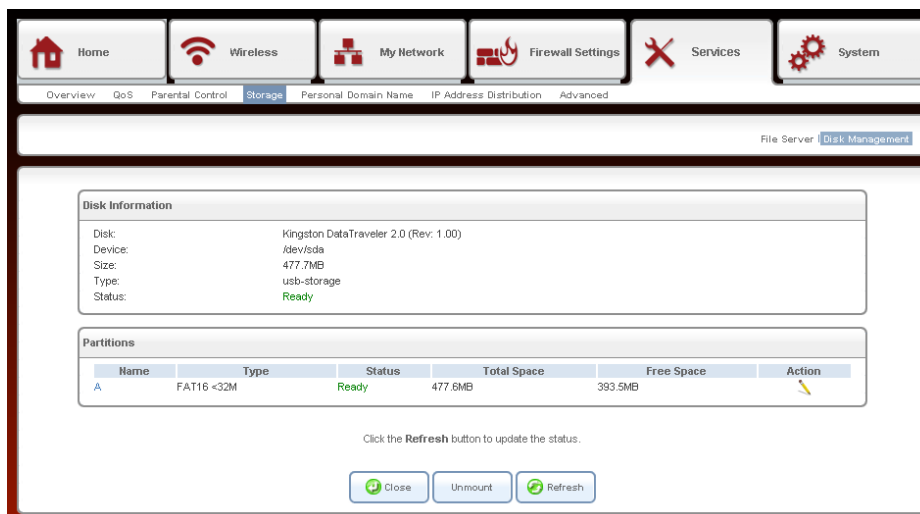
Enabled: Check to enable the disk management.

Status: Displays the status of your USB drive.

System Storage Area Status: Displays the status of the

Automatically Create System Storage Area: Check to automatically create a system storage area for your USB drive. The default partition name will be **A**. If you uncheck this box, you can rename the partition (storage area).

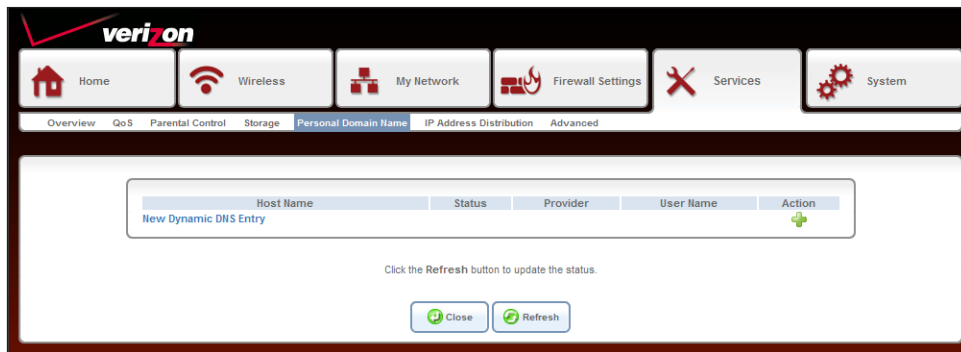
Disks: Displays information about your USB drive. Click on the Name of the drive to access more information about the drive (see below). Also, click the name under Partitions to view the files on your drive.



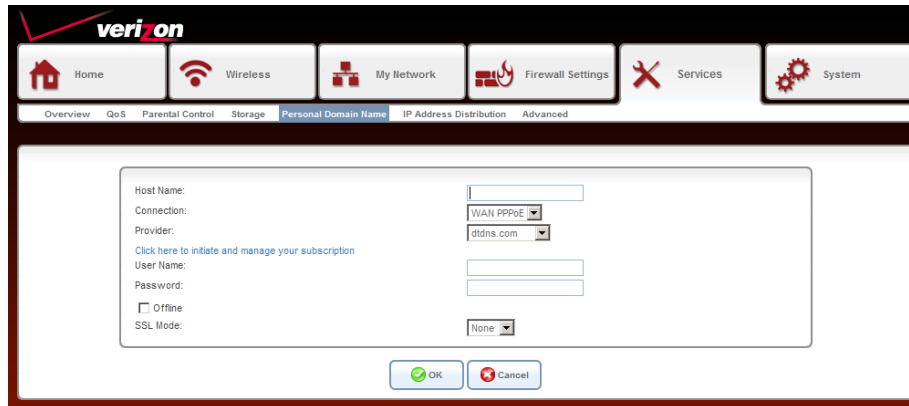
Personal Domain Name (DDNS)



Dynamic DNS is a dynamic IP address that can be aliased to a static host name, allowing a computer on the network to be more easily accessible from the Internet.



To add your DDNS information, click **New Dynamic DNS Entry**.



Host Name: Enter your full DDNS domain name (e.g. myrouter.dyndns.org).

Connection: Select the connection to which you would like to couple the DDNS service. The DDNS service will only use the chosen device, unless failover is enabled. In this case, the failed-to device will be used instead (assuming its route rules consent), until the chosen device is up again.

Provider: Select your DDNS service provider. The screen will refresh, displaying the parameters required by each provider. The provider depicted herein is dyndns, which includes all available parameters.

User Name: Enter your DDNS user name.

Password: Enter your DDNS password.

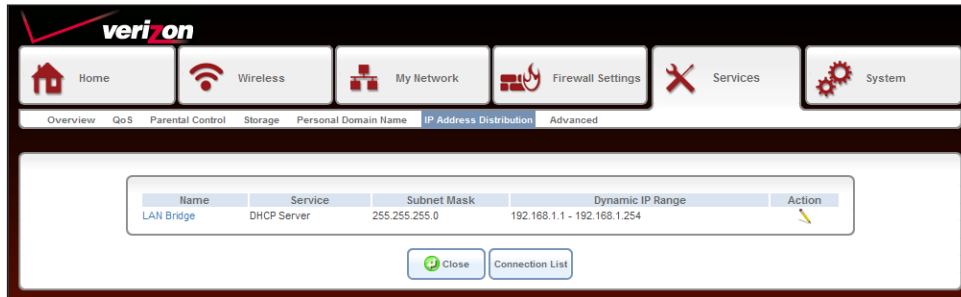
Offline: If you wish to temporarily take your site offline (prevent traffic from reaching your DDNS domain name), check this box to enable redirection of DNS requests to an alternative URL, predefined in your DDNS account. The availability of this feature depends on your account's level and type of service.

SSL Mode: With the gateway versions that support Secure Socket Layer (SSL), secured DDNS services are accessed using HTTPS. Upon connection, the gateway validates the DDNS server's certificate. Use this entry to choose the certificate's validation method.

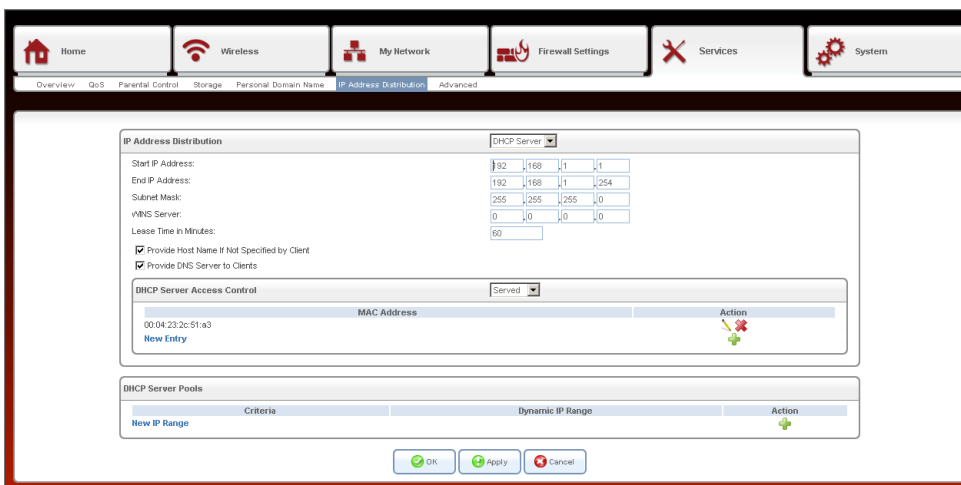
IP Address Distribution (DHCP)



Dynamic DNS is a dynamic IP address that can be aliased to a static host name, allowing a computer on the network to be more easily accessible from the Internet.



Click **LAN Bridge** to configure.



IP Address Distribution: Select DHCP Server to have your Gateway assign IP settings to your Ethernet devices connected to the LAN ports.

Start IP Address: Enter the starting IP address in your DHCP range.

End IP Address: Enter the end IP address in your DHCP range.

Subnet Mask: Enter the subnet mask of your network.

WINS Server: Enter the IP address of your WINS server (optional).

Lease Time in Minutes: Enter the lease time (in minutes).

Provide Host Name: Check this box if you want the Gateway to assign a host name to your device if one is not supplied.

Provide DNS Server: Check this box to assign the DNS server to your devices.

DHCP Server Access Control: Select **Disable** (turn off option), **Served** (to have the Gateway assign IP settings to only the devices in the list), or **Denied** (to have the Gateway assign IP settings to all devices except for the ones in the list). Click **New Entry** to add devices to the list.



System Overview

This section displays system information about the Gateway.

System Information

Gateway ID: PX2M1B800013
Software: 5.4.12.1.20 [Upgrade](#)
Version:
Release Date: Sep 15 2011
Platform: D-Link DSL-2750B Board
Tag: Ntag-5_4_12_1_20
Compilation Flags: LIC=/home/bat/bat/dlink_bcm96328_5_4_12_1/20110915_0744/conf/jpkg_bcm9636x_dlink.lic
CONFIG_RG_PROD_IMG=y DIST=DLINK_DSL2750B
System Up Time: 1 hour, 16 minutes
Load Average (1 / 0.01 / 0.01 / 0.00) 5 / 15 mins.)

Click the **Refresh** button to update the status.

[Close](#) [Refresh](#)

Settings



This section allows you to change system settings on the Gateway. It is strongly recommended not to change any of these settings. Click **Date and Time** on the right side to change the time and date on the Gateway (refer to the next page).

The screenshot shows the Verizon Gateway Settings page, specifically the System Settings section. The page has a navigation bar at the top with icons for Home, Wireless, My Network, Firewall Settings, Services, and System. Below the navigation bar, there are tabs for Overview, Settings, Users, Network Connections, Monitor, Routing, Universal Plug and Play, Maintenance, and Objects and Rules. The System Settings section is currently selected, and it contains several sub-sections:

- System:** Verizon's Hostname: verizon; Local Domain: home
- Verizon Management Console:** Automatic Refresh of System Monitoring Web Pages (checked); Warn User Before Configuration Changes (checked); Session Lifetime: 7200 Seconds
- Management Application Ports:** Primary HTTP Management Port: 80; Secondary HTTP Management Port: 8080; Primary HTTPS Management Port: 443; Secondary HTTPS Management Port: 8443; Primary Telnet Port: 23; Secondary Telnet Port: 0; Secure Telnet over SSL Port: 0
- Management Application SSL Authentication Options:** Primary HTTPS Management Client Authentication: None; Secondary HTTPS Management Client Authentication: None; Secure Telnet over SSL Client Authentication: None
- System Logging:** System Log Buffer Size: 16 KB; Remote System Notification Level: None; Persistent System Log (unchecked)
- Security Logging:** Security Log Buffer Size: 16 KB; Remote Security Notification Level: None; Persistent Security Log (unchecked)
- Swap:** Enabled (unchecked); Status: Disabled; Swap Size: 0 MB
- Host Information:** Enable Auto Detection of Host Services (checked)

At the bottom of the page, there are three buttons: OK, Apply, and Cancel.

Date and Time



This feature allows you to set the date and time values on your Gateway.

Local Time: Displays the current Gateway date and time.

Time Zone: Select your time zone from the drop-down menu.

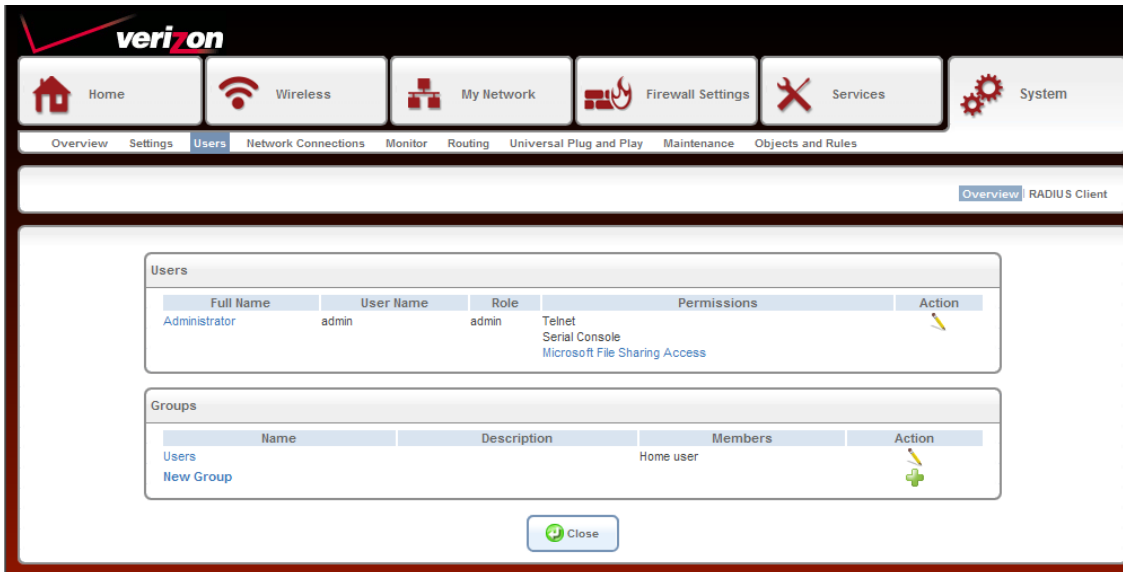
Daylight Saving Time: Check to enable daylight saving time and then enter the desired Start and End values in the fields provided. Click **Apply** to save the settings.

Automatic Time Update: Check the Enable box to use a time server. Check either TOD or NTP protocol and then enter the *Update Every* box with a value (in hours). Click **Sync Now** to connect to the server.

You may use the default server or add your own server information by clicking **New Entry**.

Users Overview

The **System** > **Users** page allows you to create users and groups, and assign permissions. Administrator is the default user.



The screenshot shows the Verizon DSL-2750B web interface. The top navigation bar includes 'Home', 'Wireless', 'My Network', 'Firewall Settings', 'Services', and 'System'. The 'System' menu is expanded, showing 'Overview', 'Settings', 'Users', 'Network Connections', 'Monitor', 'Routing', 'Universal Plug and Play', 'Maintenance', and 'Objects and Rules'. The 'Users' page is active, displaying two tables:

| Users | | | | | |
|---------------|-----------|-------|---|--------|--|
| Full Name | User Name | Role | Permissions | Action | |
| Administrator | admin | admin | Telnet Serial Console Microsoft File Sharing Access | ✎ | |

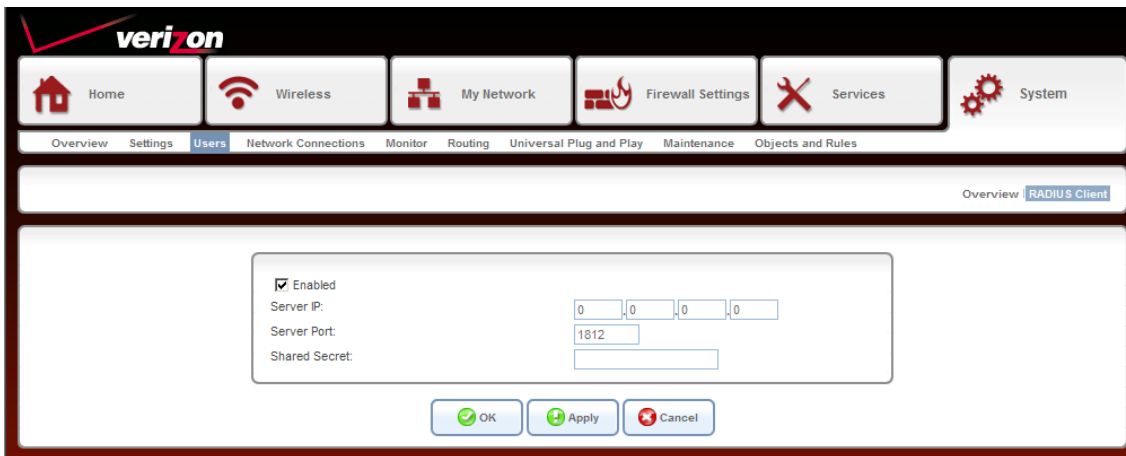
| Groups | | | | |
|---------------------------|-------------|-----------|--------|--|
| Name | Description | Members | Action | |
| Users | | Home user | ✎ | |
| New Group | | | + | |

At the bottom of the page is a 'Close' button.

Users: Displays active users, roles, and permissions. Under Action, you can click the pencil icon to edit the user's settings, the green + to add a user, or the red X to delete the user.

Groups: Displays active group, description, and members (users assign to that group). Under Action, you can click the pencil icon to edit the group's settings, the green + to add a group, or the red X to delete the group.

This page allows you to use a RADIUS server to authenticate users to log into the router.



The screenshot shows the Verizon DSL-2750B router's configuration interface. At the top, there is a navigation bar with icons for Home, Wireless, My Network, Firewall Settings, Services, and System. Below this is a secondary navigation bar with links for Overview, Settings, Users, Network Connections, Monitor, Routing, Universal Plug and Play, Maintenance, and Objects and Rules. The main content area is titled "Overview" and "RADIUS Client". It contains a form with the following fields:

- Enabled
- Server IP:
- Server Port:
- Shared Secret:

At the bottom of the form are three buttons: "OK", "Apply", and "Cancel".

Enabled: Check this box to enable RADIUS server authentication.

Server IP: Enter the IP address of the RADIUS server.

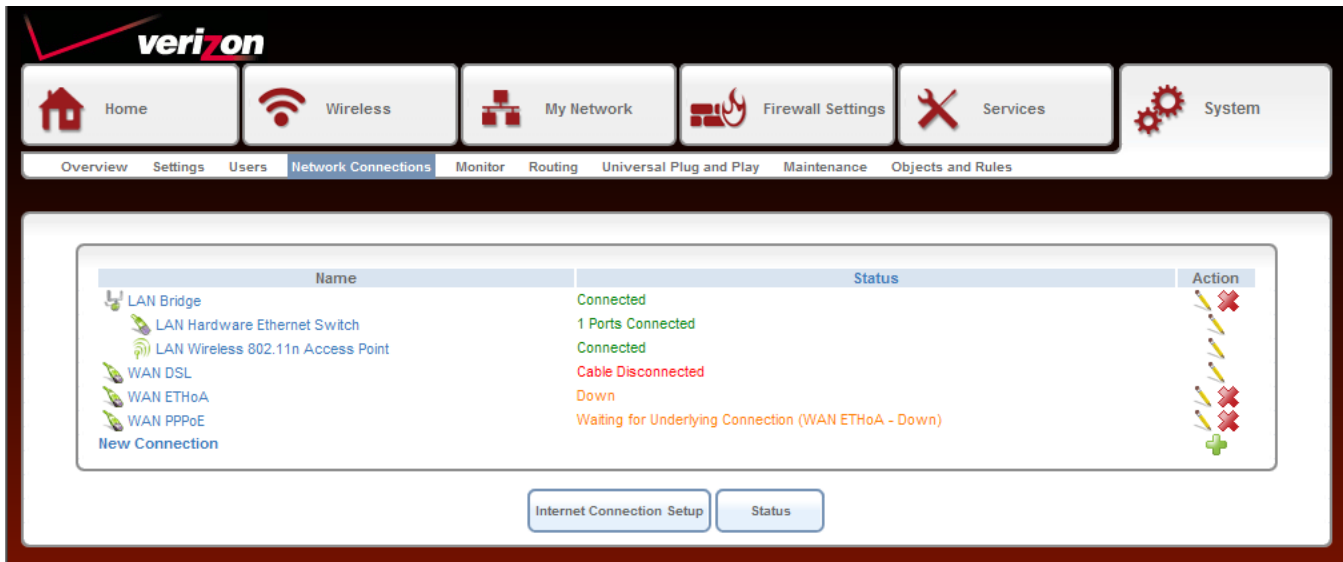
Server Port: Enter the port used.

Shared Secret: Enter the shared secret (passphrase).

Network Connections



This page will display the status of your network connections. You may add, edit, and delete these connections.



Name: Displays the name of the connection. Click on the name to edit.

Status: Displays the status of the connection.

Action: Click the pencil icon to edit the connection, the green + icon to add a new connection, or the red X to delete the connection.

New Connection: Click to add a new connection.

Monitor Network

This page will display network statistics on the Gateway.

Network CPU

| Name | LAN Bridge | LAN Wireless 802.11n Access Point | LAN Hardware Ethernet Switch | WAN DSL | WAN ETHoA | WAN PPPoE |
|-------------------------|------------------------------|-----------------------------------|------------------------------|--------------------|-------------------|--|
| Device Name | br0 | wl0 | bcmsw | bcm_atm0 | etho0 | ppp0 |
| Status | Connected | Connected | 1 Ports Connected | Cable Disconnected | Down | Waiting for Underlying Connection (WAN ETHoA - Down) |
| Network | LAN | LAN | LAN | WAN | WAN | WAN |
| Underlying Device | LAN Hardware Ethernet Switch | LAN Wireless 802.11n Access Point | LAN Hardware Ethernet Switch | DSL | WAN DSL | WAN ETHoA |
| Connection Type | Bridge | Wireless 802.11n Access Point | Hardware Ethernet Switch | DSL | ETHoA | PPPoE |
| Download Rate | 100.0 Mbps | 130.0 Mbps | 100.0 Mbps | | | |
| Upload Rate | 100.0 Mbps | 130.0 Mbps | 100.0 Mbps | | | |
| MAC Address | 00:26:5a:49:3e:08 | 00:26:5a:49:3e:0a | 00:26:5a:49:3e:0b | | 00:26:5a:49:3e:09 | |
| IP Address | 192.168.1.1 | | | | | |
| Subnet Mask | 255.255.255.0 | | | | | |
| IP Address Distribution | DHCP Server | Disabled | Disabled | | Disabled | |
| Service Name | | | | | | |
| User Name | | | | | | newdal |
| VPLVCI | | | | | 0.35 | 0.35 |
| Encryption | | WPA2 | | | | |
| Received Packets | 13871 | 0 | 0 | | | |
| Sent Packets | 17557 | 0 | 3554 | | | |
| Received Bytes | 1897732 | 0 | 0 | | | |
| Sent Bytes | 19222200 | 0 | 460784 | | | |
| Receive Errors | 0 | 17 | 0 | | | |
| Receive Drops | 0 | 0 | 0 | | | |
| Time Span | 1:20:24 | 1:05:27 | 1:20:24 | | | |

Click the Refresh button to update the status.

Close Automatic Refresh Off Reset Statistics Refresh

CPU

This page will display the Gateway's CPU statistics.

Network CPU

Gateway ID: PX2M1B0000013

System Up Time: 1 hour, 21 minutes

Load Average (1 / 5 / 15 mins.): 0.00 / 0.00 / 0.00

Processes

| Process | Total Virtual Memory (VmData) | Heap size (VmSize) |
|-------------|-------------------------------|--------------------|
| init | 152 kB | 700 kB |
| openrg | 2448 kB | 8692 kB |
| smbd | 832 kB | 4632 kB |
| nmbd | 736 kB | 2148 kB |
| smbd | 832 kB | 4632 kB |
| nas | 176 kB | 748 kB |
| wps_monitor | 480 kB | 2816 kB |
| eapd | 100 kB | 576 kB |

Click the Refresh button to update the status.

Close Automatic Refresh Off Refresh

Routing Overview



Routing Table

| Name | Destination | Gateway | Netmask | Metric | Status | Action |
|---------------------------|-------------|---------|---------|--------|--------|--------|
| New Route | | | | | | |

Internet Group Management Protocol (IGMP) Enabled

IGMP Fast Leave
 IGMP Multicast to Unicast

The routing table will display any routes. Check the IGMP Enabled box and check to enable IGMP Fast Leave and/or IGMP Multicast to Unicast. Click **OK** to save your settings.

PPPoE Relay

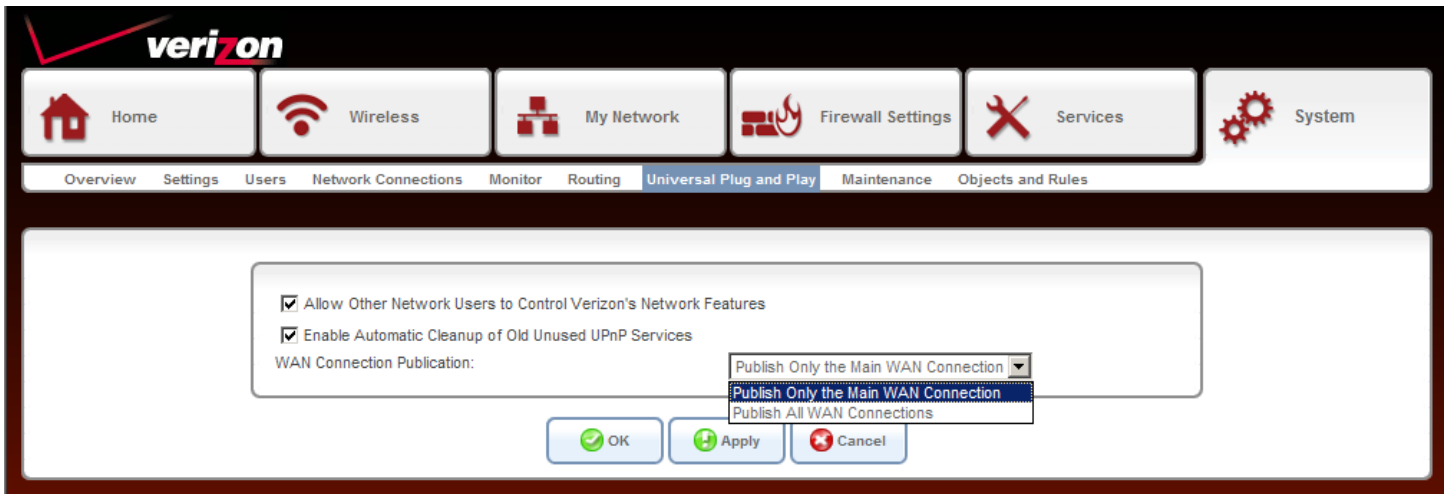
Overview > Settings > Users > Network Connections > Monitor > Routing > Universal Plug and Play > Maintenance > Objects and Rules

Overview > PPPoE Relay

Enabled

Check the Enabled box to activate PPPoE relay. Click **OK** to save your settings.

Universal Plug and Play (UPnP™)



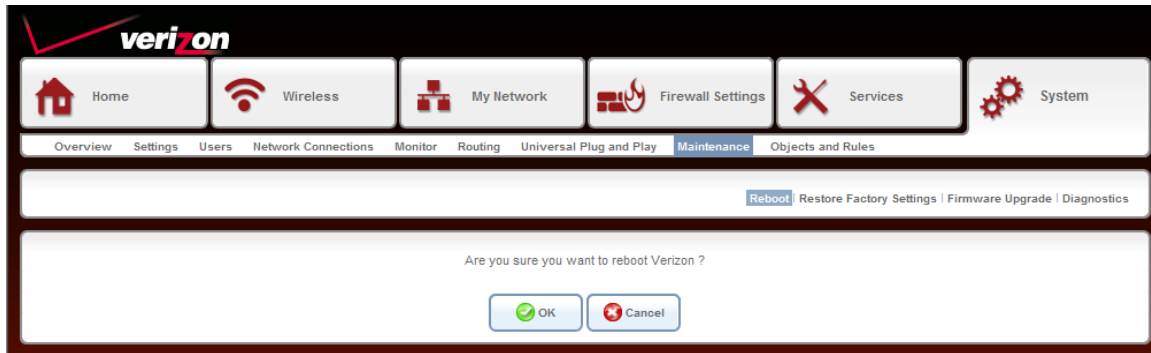
Allow Other Network Users to Control Verizon's Network Features: Check this box to broadcast the router to all computers on your local network. Your computer (if UPnP is enabled on your computer) will detect the router as a UPnP device.

Enable Automatic Cleanup of Old Unused UPnP Services: Check this box to have the Gateway automatically remove unused UPnP services.

WAN Connection Publication: Select **Publish Only the Main WAN Connection**.

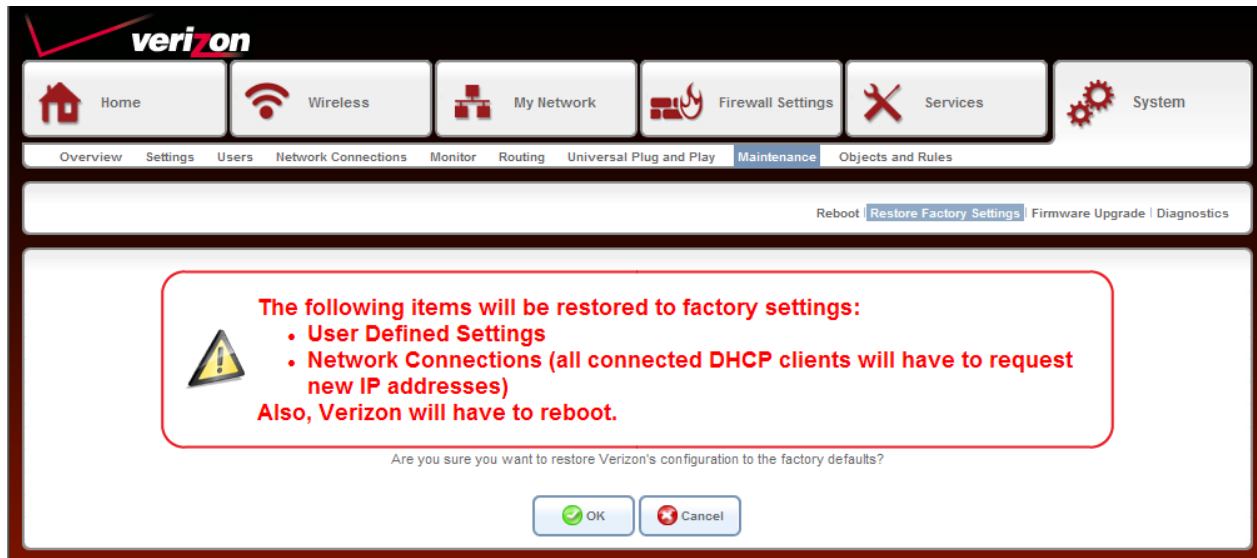
OK: Click **OK** to save your settings.

Maintenance Reboot

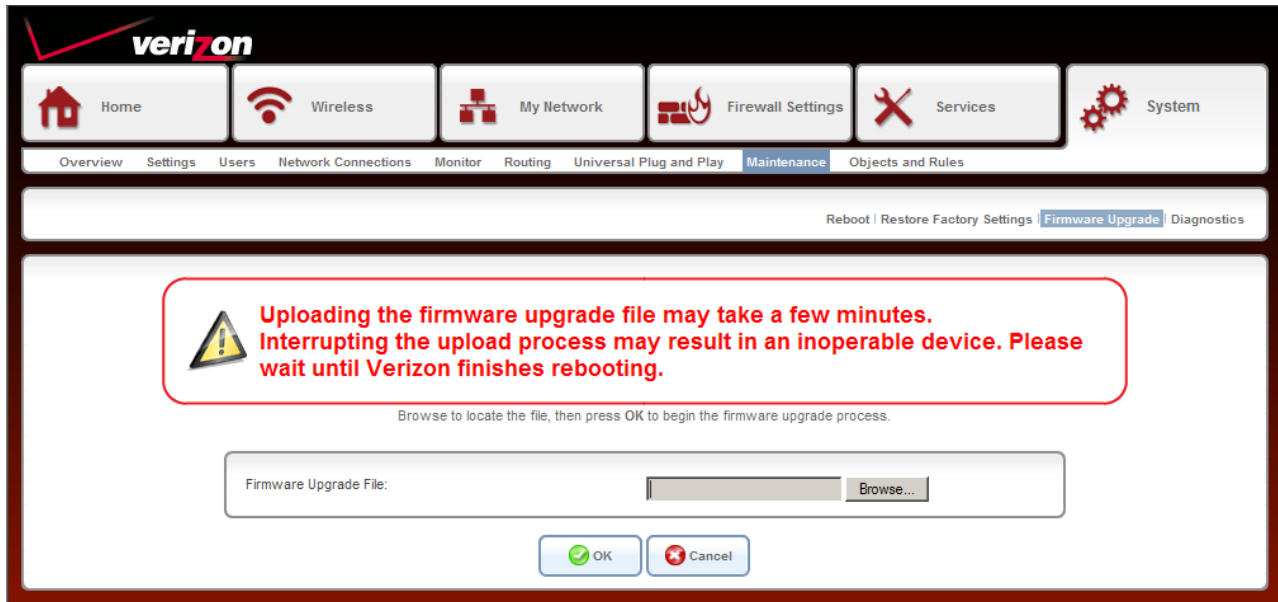


Click **OK** to reboot the Gateway.

Restore Factory Settings



Click **OK** to reset the Gateway to the default factory settings. All rules, users, groups, etc you configured will be lost.



Visit the Verizon website to download a firmware upgrade file to your computer if available. Click **Browse** and then navigate to the location of the upgrade file; the path will appear in the window. Next, click **OK** to begin the upload to your Gateway.

Diagnostics



This page will allow you to test different connection using Ping, ARP, Traceroute, PVC Scan, and OAM Ping. Enter the IP address of your target (destination) and adjust settings if needed, then click **Go**. The results will appear next to *Status*.

| | | |
|-------------------------|---|-----------------------------------|
| Ping (ICMP Echo) | | |
| Destination: | <input type="text"/> | <input type="button" value="Go"/> |
| Number of pings: | <input type="text" value="4"/> | |
| Status: | | |
| ARP | | |
| Destination: | <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> | <input type="button" value="Go"/> |
| Status: | | |
| Traceroute | | |
| Destination: | <input type="text"/> | <input type="button" value="Go"/> |
| Status: | | |
| PVC Scan | | |
| Status: | | <input type="button" value="Go"/> |
| OAM Ping | | |
| Type: | <input type="text" value="F4 End-to-End"/> | <input type="button" value="Go"/> |
| VPI: | <input type="text" value="0"/> | |
| VCI: | <input type="text" value="4"/> | |
| Count: | <input type="text" value="0"/> | |
| Status: | | |















Click the **Refresh** button to update the status.

Objects and Rules

Protocols



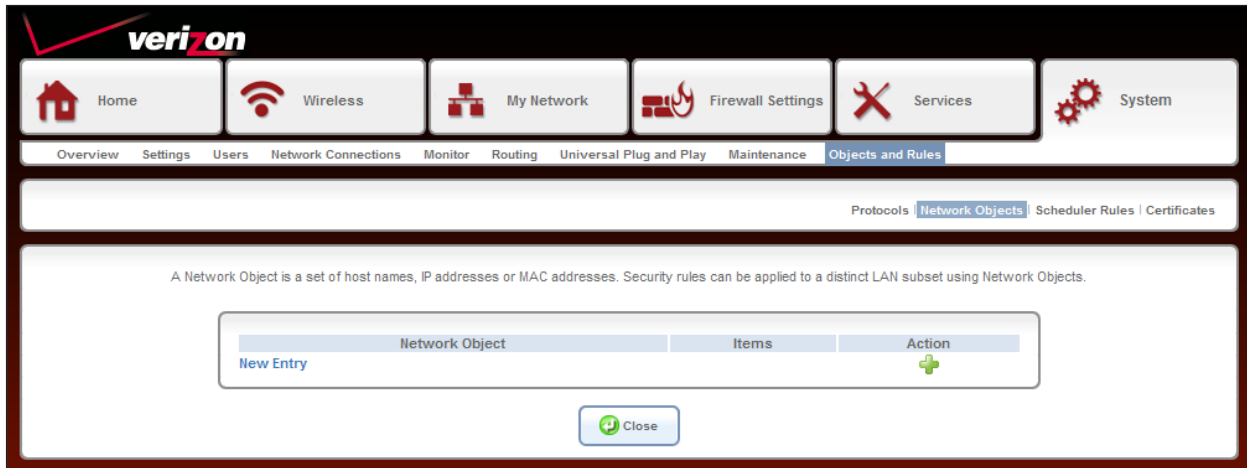
The Protocols page will display all the default and user-created services and their port information. This is used for the Port Forwarding and Port Triggering features. You may click the pencil icon to edit the item, click the red X to remove the item, or scroll all the way to the bottom and click **New Entry** on the left side to create a new protocol.

| Protocols | Ports | Action |
|------------------------------|----------------------|---|
| Age of Empires (I, II & III) | TCP Any -> 23978 |   |
| | Any -> 80 | |
| | Any -> 23 | |
| | Any -> 2300-2400 | |
| | Any -> 47624 | |
| | UDP Any -> 23978 | |
| AIM / AOL ICQ | Any -> 6073 |   |
| | Any -> 2300-2400 | |
| | TCP Any -> 5190 | |
| AIM Talk | UDP Any -> 5190 |   |
| | TCP Any -> 4099 | |
| Aliens vs. Predator | TCP Any -> 80 |   |
| | Any -> 2300-2400 | |
| | Any -> 8000-8999 | |
| | UDP Any -> 80 | |
| America's Army | Any -> 2300-2400 |   |
| | Any -> 8000-8999 | |
| | TCP Any -> 14200 | |
| | Any -> 20025-20048 | |
| AOL | UDP Any -> 1716-1718 |   |
| | Any -> 8777 | |
| | Any -> 27900 | |
| | TCP Any -> 5190-5193 |   |
| | UDP Any -> 5190-5193 | |

Network Objects



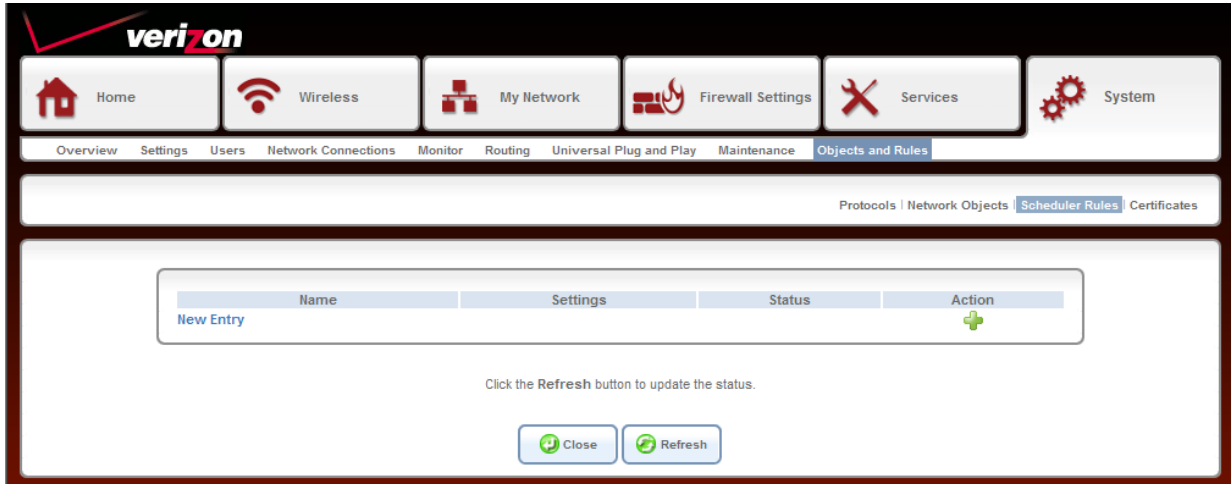
Network objects are devices on your local network such as computers, game consoles, media players, Internet TVs, and network storage (NAS) devices, or a specific IP address or a range of IP address. You can add a network object by clicking **New Entry**.



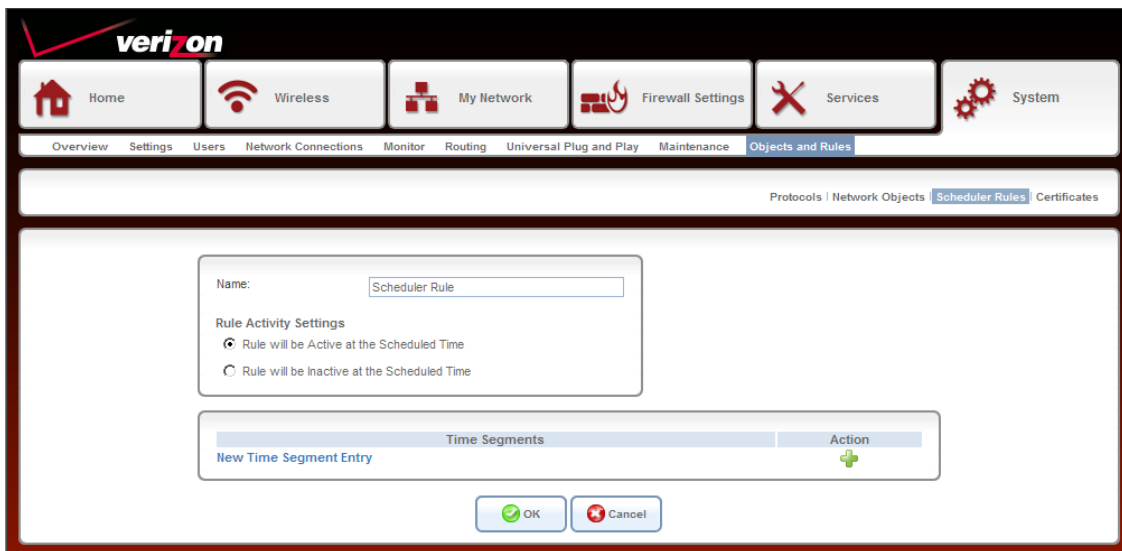
Scheduler Rules



Scheduler Rules will allow you to set up a specific schedule that you can apply to parental control and firewall features. For example if you want to block your kids' computers from the Internet at certain times, you can create a schedule that specifies the day and time you want blocked, and then apply that schedule to a firewall rule. Click **New Entry** or the green + icon.



Click **New Entry** or the green + icon under *Action* and the following screen will appear.



Name: Enter a name for your rule.

Rule Activity Settings: Select either the time frame is going to be active or inactive.

New Time Segment Entry: Click to enter the time frame you want for the rule.

OK: Click to save your rule.

Certificates



verizon

Home Wireless My Network Firewall Settings Services System

Overview Settings Users Network Connections Monitor Routing Universal Plug and Play Maintenance **Objects and Rules**

Protocols | Network Objects | Scheduler Rules **Certificates**

Verizon's Local CA's

| Name | Issuer | Action |
|-----------------------|-------------------|--------|
| Verizon | C=US, CN=Jungo CA | |
| Verizon remote update | C=US, CN=Jungo CA | |

[Upload Certificate](#)

[Close](#) [Create Certificate Request](#) [Create Self Signed Certificate](#)

verizon

Home Wireless My Network Firewall Settings Services System

Overview Settings Users Network Connections Monitor Routing Universal Plug and Play Maintenance **Objects and Rules**

Protocols | Network Objects | Scheduler Rules **Certificates**

Verizon's Local CA's

| Name | Issuer | Action |
|-----------------|---|--------|
| Jungo Root CA | C=US, CN=Jungo CA | |
| Jungo Root CA2 | C=IL, ST=HaMerkaz, L=Netanya, O=Jungo CA, OU=IT CA, CN=Jungo Root CA, emailAddress=yarony@jungo.com | |
| D-Link ADSL CA | C=E, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root | |
| D-Link ADSL CA2 | C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority | |

[Upload Certificate](#)

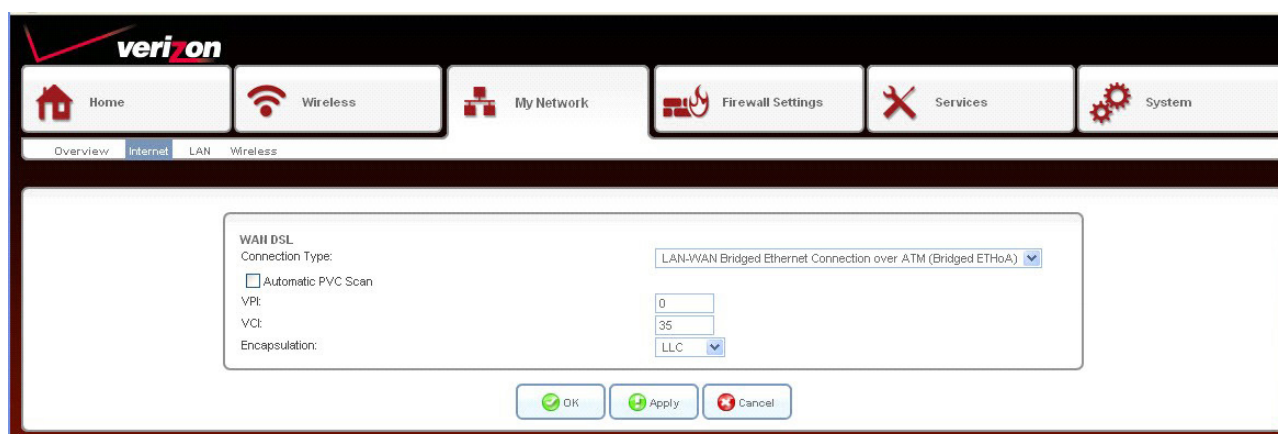
[Close](#)

Advanced Configuration

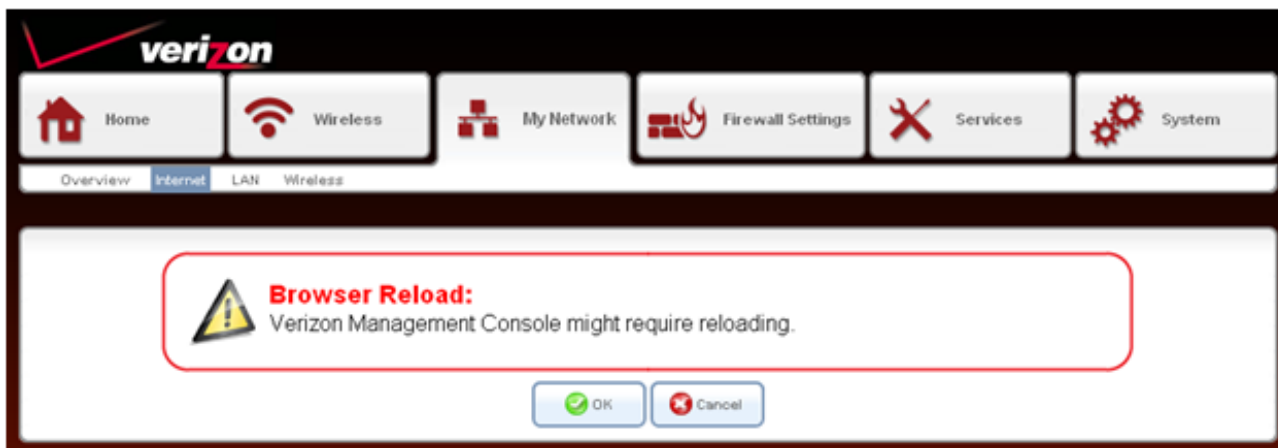
Bridge Mode

Before following the steps below, please factory reset the DSL-2750B. After it has booted up, disable the Wireless by depressing the button on the back of the unit. Complete the following steps to set up Bridge mode on the DSL-2750B:

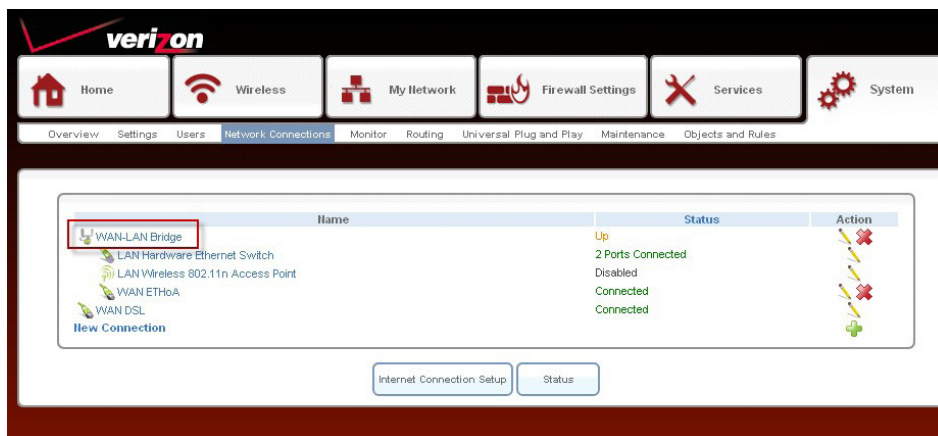
1. Open a web browser and enter **http://192.168.1.1**.
2. Log in with the default user name (**admin**) and password (refer to back label of 2750B).
3. Select **My Network > Internet**.
4. From the drop-down menu next to *Connection type*, select **LAN-WAN Bridged Ethernet Connection over ATM (Bridged ETHoA)**.



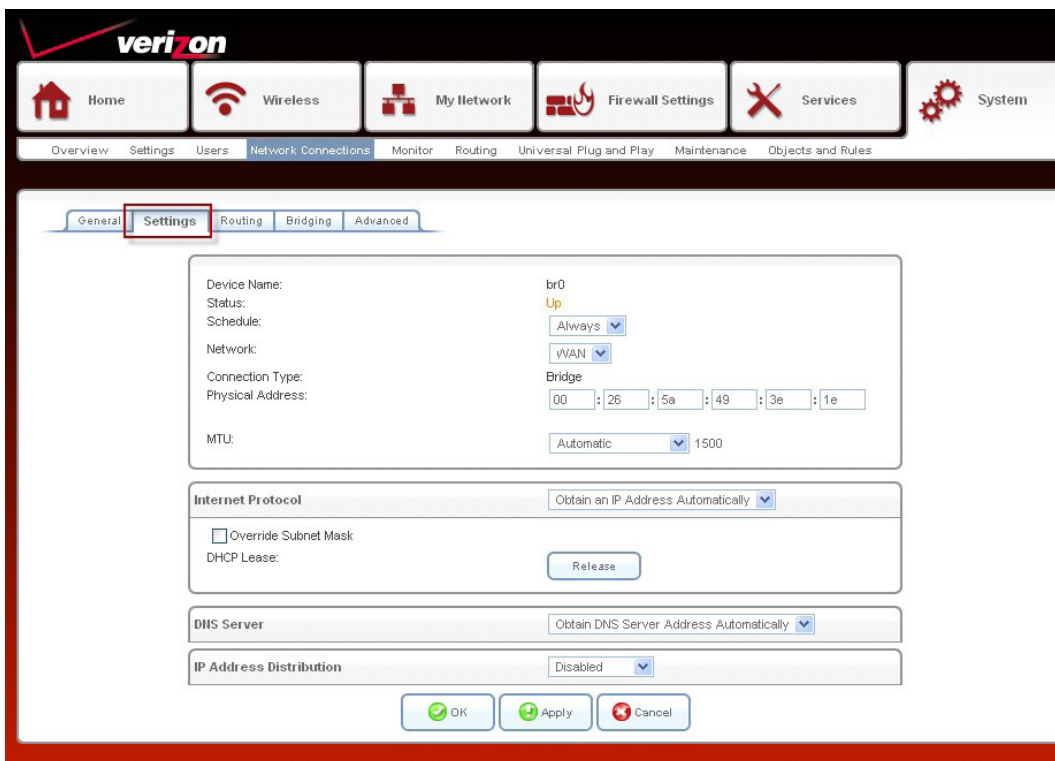
5. Click **Apply**.
6. When the following message appears, click **OK**.



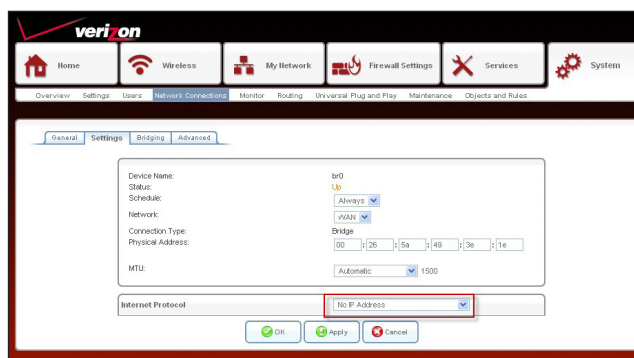
7. Browse to **System > Network Connections** and click **WAN-LAN Bridge**.



8. Click the **Settings** tab.



9. Under *Internet Protocol*, change the setting to **No IP Address**. Click **Apply**.

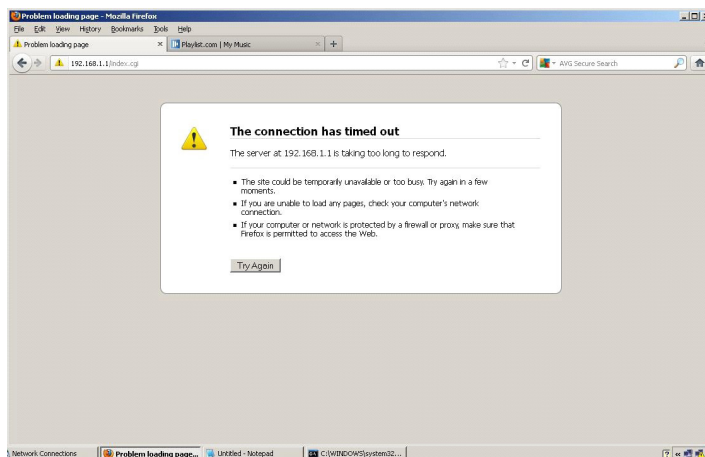


10. When the Browser Reload message appears, click **OK**.

11. The following settings take place once the DSL-2750B is in Bridge mode:

- a. VPI/VCI: 0/35
- b. Encapsulation: LLC
- c. DHCP server is disabled for both wired/wireless clients
- d. GUI is accessible only through 192.168.1.1 by a PC configured with static IP address of 192.168.1.x/24.

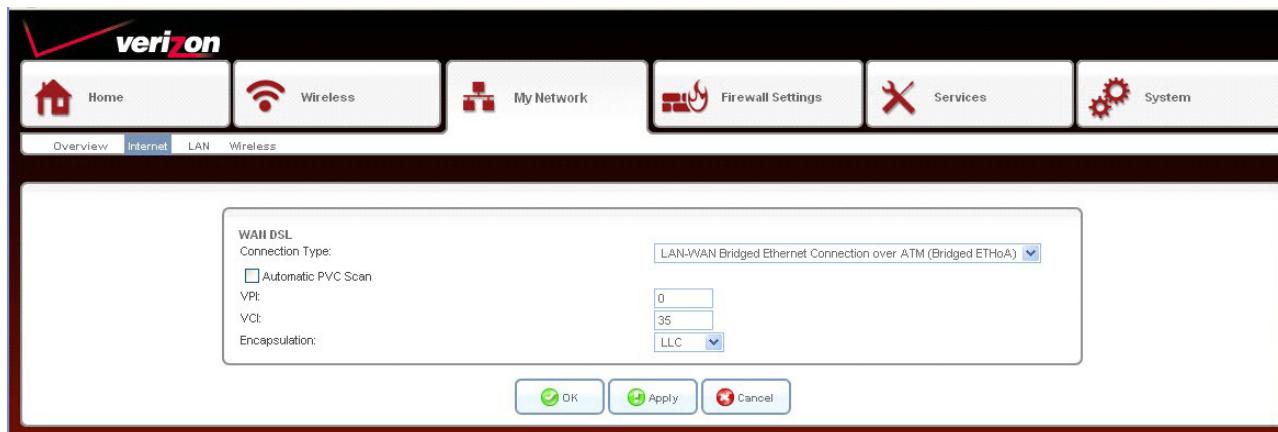
Note: Once you have configured the DSL-2750B for Bridge mode, release and renew your network adapter cards. On a DHCP line, your PC will now receive a public IP address. On a PPPoE line, you should receive a 169.254.x.x IP address. The GUI will not be accessible and you should get the following message when trying to do so.



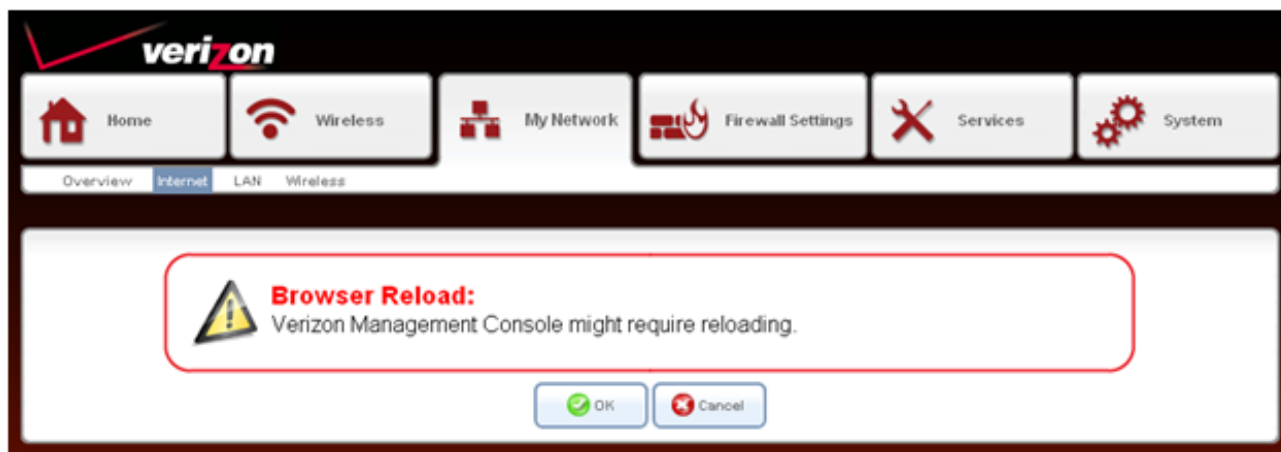
Multiple Static Public IPs

Before following the steps below, please factory reset the DSL-2750B.

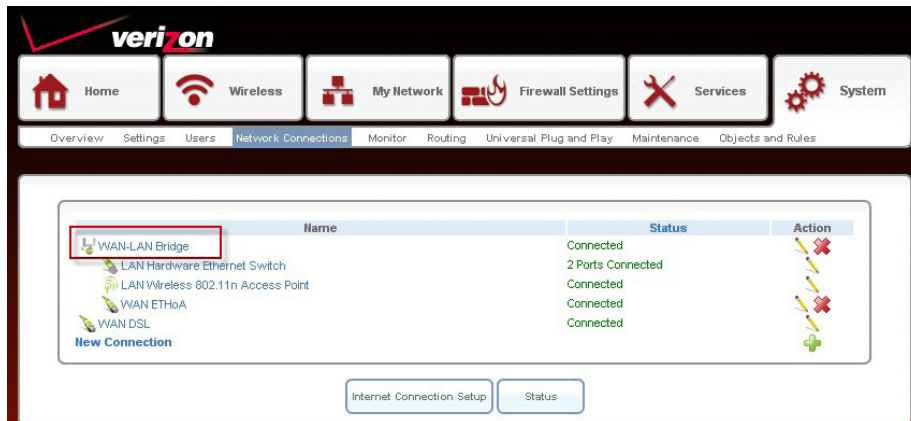
1. Open a web browser and enter **http://192.168.1.1**.
2. Log in with the default user name (**admin**) and password (refer to back label of 2750B).
3. Select **My Network > Internet**.
4. From the drop-down menu next to *Connection type*, select **LAN-WAN Bridged Ethernet Connection over ATM (Bridged ETHoA)**.



5. Click **Apply**.
6. When the following message appears, click **OK**.

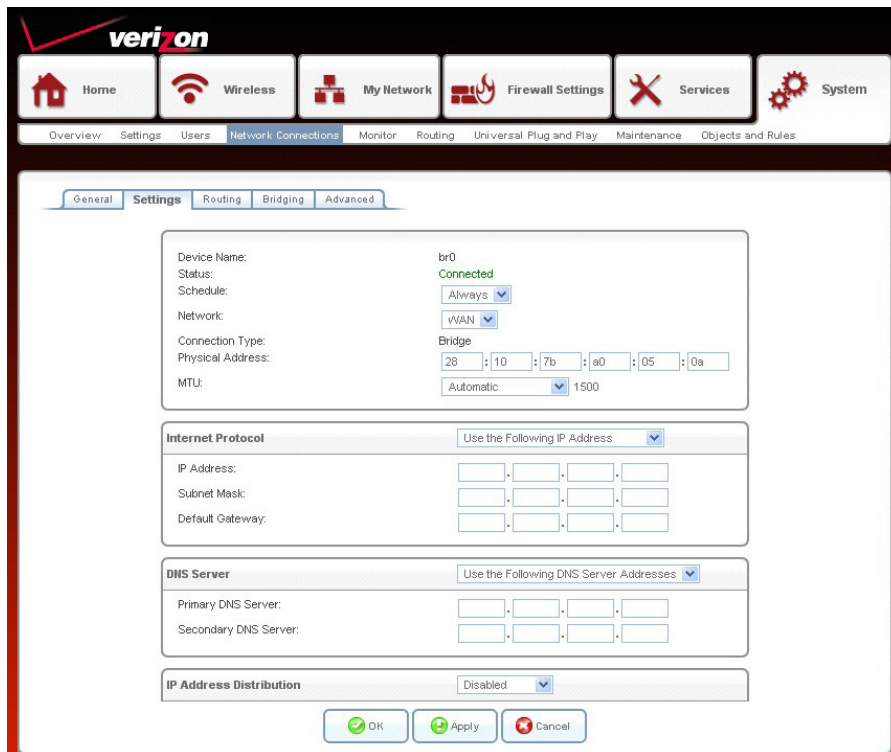


7. Click **System** > **Network Connections** > **WAN-LAN Bridge**.

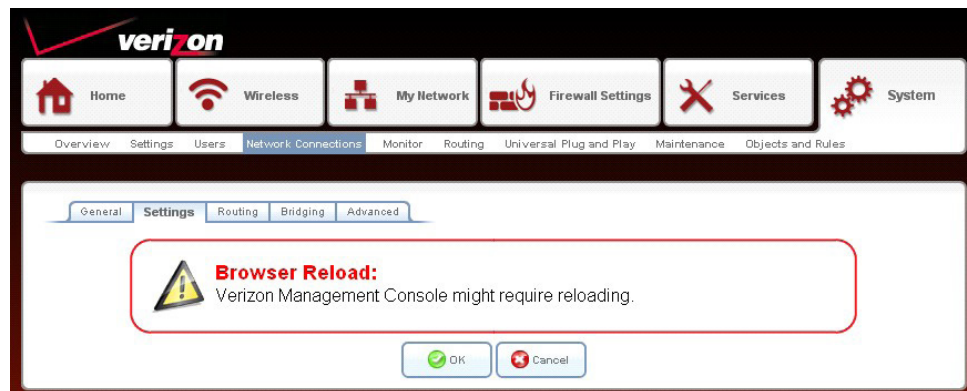


8. Click **Settings**.

9. From the drop-down menu next to *Internet Protocol*, select **Use the Following IP Address**.
- a. This will give you the option to input the static IP Address, Subnet, Gateway and DNS.
 - b. Enter your information and click **Apply**.



10. When the following message appears, click **OK**.



11. Additional Public IP Addresses can be statically configured on LAN PCs.

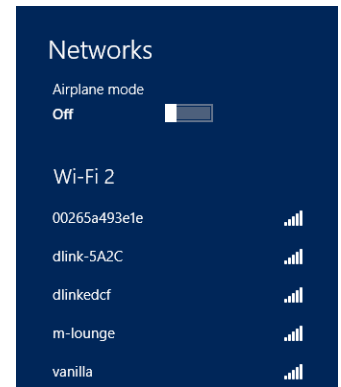
Connect to your Wireless Network



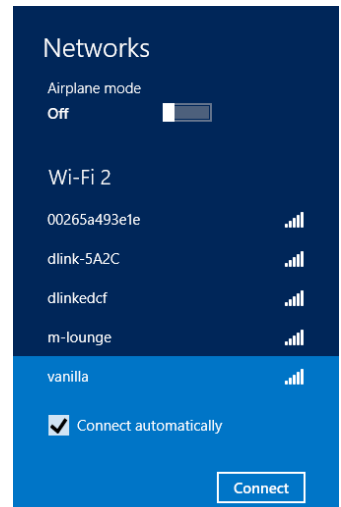
Windows® 8

1. Click on the wireless computer icon in your system tray (lower-right corner next to the time).

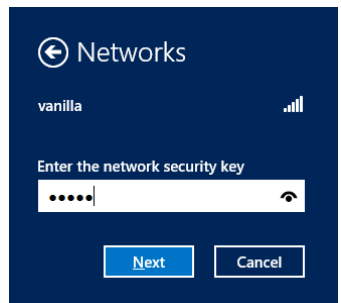
2. A list of available wireless networks will appear.



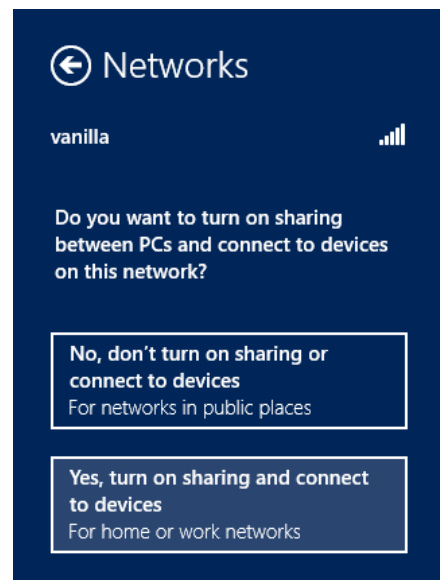
3. Click the wireless network (SSID) you want to connect to and then click **Connect**.



4. If the network is secure/encrypted, enter the Wi-Fi password (security key) and click **Next**.



5. Click either to enable or disable file sharing.
6. You will now be connected to your wireless network.



If you get a good signal but cannot access the Internet, confirm the encryption by reviewing the profile or check the TCP/IP settings for your wireless adapter. Refer to the *Networking Basics* section in this manual for more information.

It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the passphrase being used.

1. Click on the wireless icon in your system tray (lower-right corner).



Wireless Icon

2. The utility will display any available wireless networks in your area.

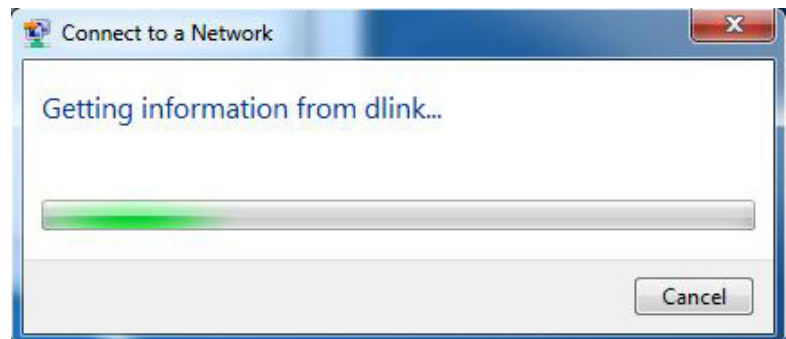


3. Highlight the wireless network (SSID) you would like to connect to and click the **Connect** button.

If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.

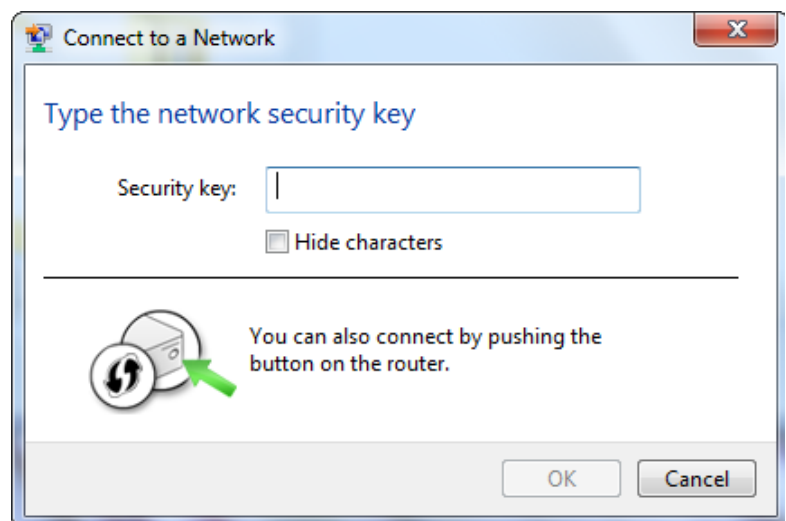


4. The following window appears while your computer tries to connect to the Gateway.



5. Enter the same passphrase that is on your Gateway and click **Ok**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The passphrase must be exactly the same as on the Gateway.

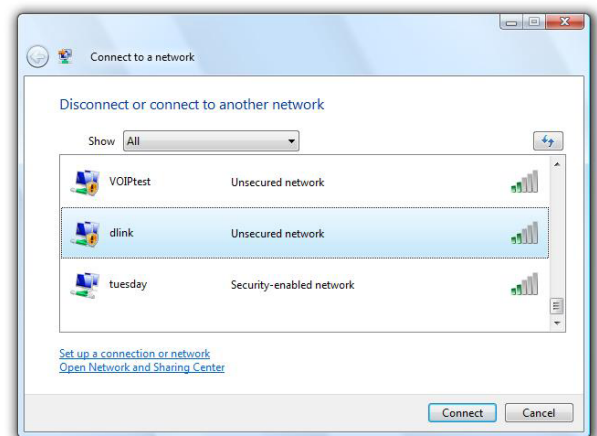


Windows Vista® users may use the built-in wireless utility. If you are using another company's utility please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows Vista® utility as seen below.

1. Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **Connect to a network**.

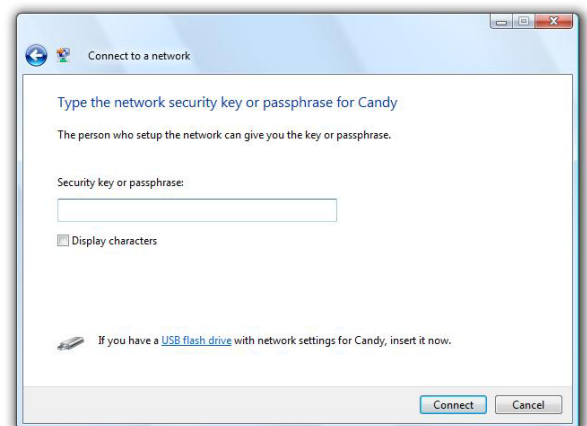


2. The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.



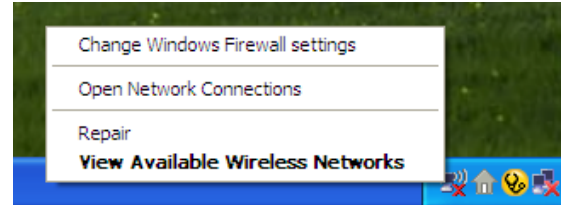
3. Enter the same security key or passphrase that is on your router and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.

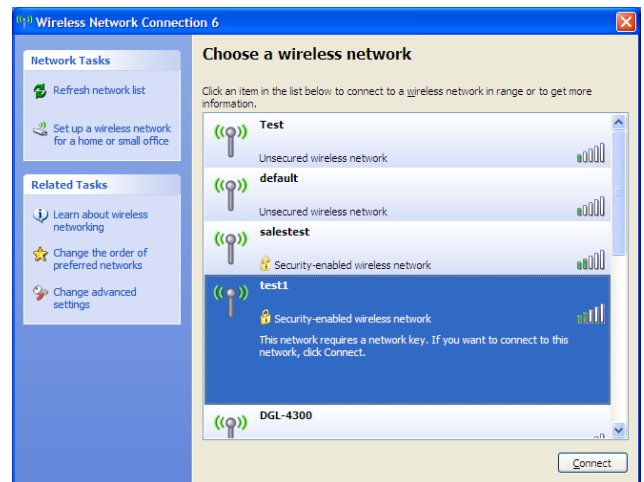


Windows® XP users may use the built-in wireless utility. If you are using another company's utility, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows® XP utility as seen below.

1. Right-click on the wireless computer icon in your system tray (lower right corner next to the time). Select **View Available Wireless Networks**.

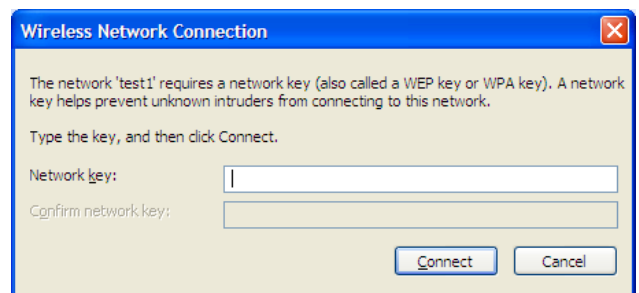


2. The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.



3. The **Wireless Network Connection** box will appear. Enter the WPA/WPA2 passphrase and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WPA/WPA2 settings are correct. The WPA/WPA2 passphrase must be exactly the same as on the wireless router.



Networking Basics



Check your IP address

After you install your new D-Link wireless adapter and have established a wireless connection, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e., router) automatically. To verify your IP address, please follow the steps below.

Windows® 8 Users

- Press the **Windows key** and **R** together. Type **cmd** in the box and click **OK**.
- At the prompt, type **ipconfig** and press **Enter**.
- This will display the IP address, subnet mask, and default gateway of your adapter.

```
Administrator: E:\Windows\system32\cmd.exe
E:\Users\Admin>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : public.palab
    Link-local IPv6 Address . . . . . : fe80::a9e34e33f8f6:478ax0
    IPv4 Address. . . . . : 192.168.0.197
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Tunnel adapter Local Area Connection* 14:

    Connection-specific DNS Suffix  . : public.palab
    Link-local IPv6 Address . . . . . : fe80::5efe:192.168.0.197:20
    Default Gateway . . . . . :

Tunnel adapter Local Area Connection* 7:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

E:\Users\Admin>
```

Windows® 7/Vista® Users

- Click **Start**, type **cmd** in the search box and then click **OK**.
- At the prompt, type **ipconfig** and press **Enter**.
- This will display the IP address, subnet mask, and default gateway of your adapter.

Windows® XP Users

- Click on **Start** > **Run**. In the run box type **cmd** and click **OK**.
- At the prompt, type **ipconfig** and press **Enter**.
- This will display the IP address, subnet mask, and the default gateway of your adapter.

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.

Statically Assign an IP Address

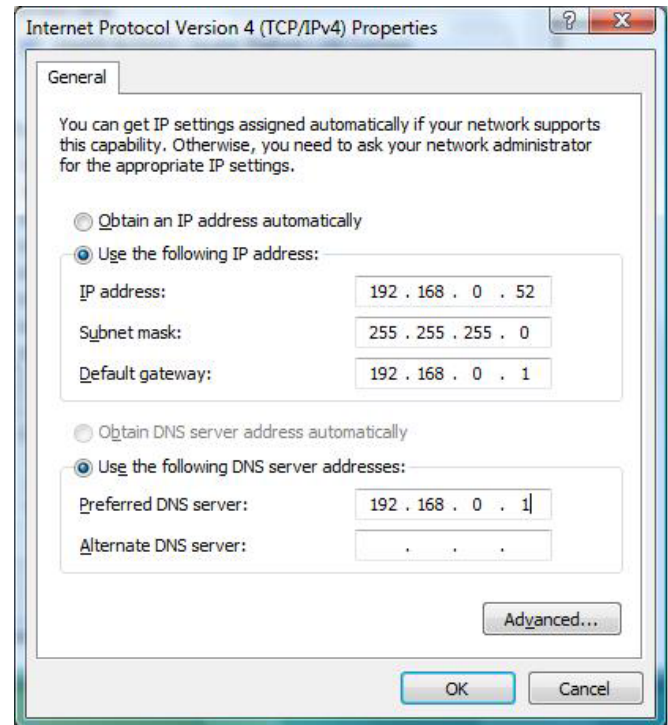


If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

Windows® 8 Users

- Press the **Windows** key and then type **IP**. Click **Settings** on the right side and then click **View Network Connections**.
- Right-click on the adapter which represents your wireless network adapter.
- Highlight **Internet Protocol Version 4 (TCP /IPv4)** and click **Properties**.
- Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or LAN IP address on your router or network.

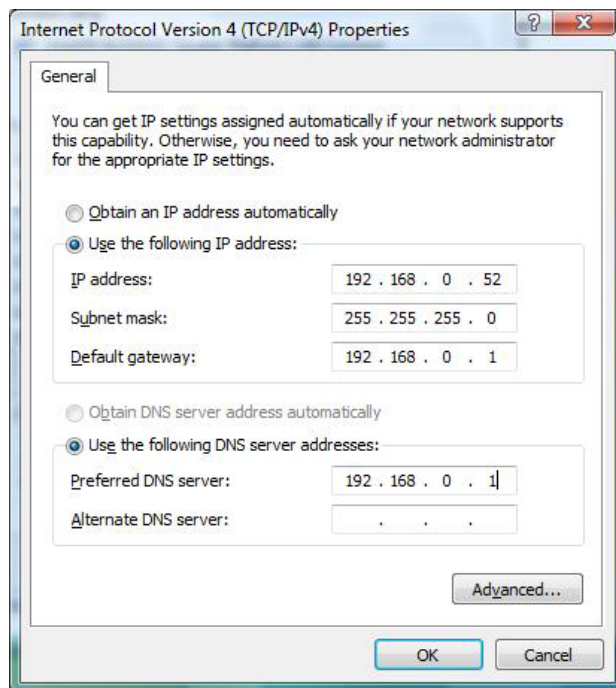
Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network.



- Set **Default Gateway** the same as the LAN IP address of your router or gateway.
- Set **Primary DNS** the same as the LAN IP address of your router or gateway.
- The **Secondary DNS** is optional (you may enter a DNS server from your ISP).
- Click **OK** to save your settings.

Windows® 7/ Vista® Users

- Click on **Start > Control Panel** (make sure you are in Classic View). Double-click on the **Network and Sharing Center** icon. If you are using Windows Vista, click on **Manage network connections** along the left panel in the window. For Windows® 7, click on **Change adapter settings**.
- Right-click on the **Local Area Connection** which represents your wireless network adapter which will be connected to your network.
- Highlight **Internet Protocol Version 4 (TCP /IPv4)** and click **Properties**.
- Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or LAN IP address on your router or network.



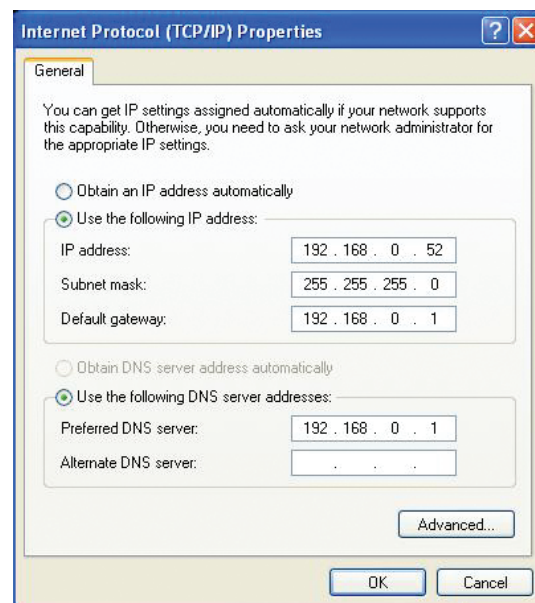
Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network.

- Set **Default Gateway** the same as the LAN IP address of your router or gateway.
- Set **Primary DNS** the same as the LAN IP address of your router or gateway.
- The **Secondary DNS** is optional (you may enter a DNS server from your ISP).
- Click **OK** to save your settings.

Windows® XP Users

- Click on **Start > Control Panel**. Make sure you are in Classic View. Double-click on the Network Connections icon.
- Right-click on the Local Area Connection which represents your wireless network adapter.
- Highlight *Internet Protocol (TCP/IP)* and click **Properties**.
- Click **Use the following IP address** and enter an IP address that is on the same subnet as your network.

Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network.



- Set **Default Gateway** the same as the LAN IP address of your router or gateway.
- Set **Primary DNS** as the LAN IP address of your router or gateway.
- The **Secondary DNS** is optional (you may enter a DNS server from your ISP).
- Click **OK** to save your settings.